

H A N D B O O K O F

MATHEMATICAL
LOGIC

Edited by JON BARWISE

N O R T H - H O L L A N D

HANDBOOK OF MATHEMATICAL LOGIC

STUDIES IN LOGIC AND THE FOUNDATIONS OF MATHEMATICS

VOLUME 90

Editors

H. J. KEISLER, *Madison*
A. MOSTOWSKI†, *Warszawa*
A. ROBINSON†, *New Haven*

erdam

d

Y. BAR-HILLEL†, *Jerusalem*
K. L. DE BOUVÈRE, *Santa Clara*
H. HERMES, *Freiburg i. Br.*
J. HINTIKKA, *Helsinki*
J. C. SHEPHERDSON, *Bristol*
E. P. SPECKER, *Zürich*

ELSEVIER

AMSTERDAM • LAUSANNE • NEW YORK • OXFORD • SHANNON • SINGAPORE • TOKY

HANDBOOK OF MATHEMATICAL LOGIC

EDITED BY

JON BARWISE

University of Wisconsin, Madison



ELSEVIER

AMSTERDAM • LAUSANNE • NEW YORK • OXFORD • SHANNON • SINGAPORE • TOKYO

ELSEVIER SCIENCE B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

First edition: 1977
Second impression: 1978
Third impression: 1983
Fourth impression: 1985

Fifth impression: 1989
Sixth impression: 1991
Seventh impression: 1991
Eighth impression: 1999

Library of Congress Cataloging-in-Publication Data

Main entry under title:
Handbook of mathematical logic.

(Studies in logic and the foundations of mathematics; 90)

Includes index.

I. Logic, Symbolic and mathematical. I. Barwise, Jon. II. Keisler, H. Jerome. III. Series.

QA9. H32 511'.3 76-26032

ISBN: 0-7204-2285-X

ISBN: 0-444-86388-5 (PB)

© 1977 Elsevier Science B.V. All rights reserved.

This work is protected under copyright by Elsevier Science, and the following terms and conditions apply to its use:

Photocopying

Single photocopies of single chapters may be made for personal use as allowed by national copyright laws. Permission of the publisher and payment of a fee is required for all other photocopying, including multiple or systematic copying, copying for advertising or promotional purposes, resale, and all forms of document delivery. Special rates are available for educational institutions that wish to make photocopies for non-profit educational classroom use.

Permissions may be sought directly from Elsevier Science Rights & Permissions Department, PO Box 800, Oxford OX5 1DX, UK; phone: (+44) 1865 843830, fax: (+44) 1865 853333, e-mail: permissions@elsevier.co.uk. You may also contact Rights & Permissions directly through Elsevier's home page (<http://www.elsevier.nl>), selecting first 'Customer Support', then 'General Information', then 'Permissions Query Form'.

In the USA, users may clear permissions and make payments through the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, USA; phone: (978) 7508400, fax: (978) 7504744, and in the UK through the Copyright Licensing Agency Rapid Clearance Service (CLARCS), 90 Tottenham Court Road, London W1P 0LP, UK; phone: (+44) 171 436 5931; fax: (+44) 171 436 3986. Other countries may have a local reprographic rights agency for payments.

Derivative Works

Tables of contents may be reproduced for internal circulation, but permission of Elsevier Science is required for external resale or distribution of such material.

Permission of the publisher is required for all other derivative works, including compilations and translations.

Electronic Storage or Usage

Permission of the publisher is required to store or use electronically any material contained in this work, including any chapter or part of a chapter. Contact the publisher at the address indicated.

Except as outlined above, no part of this work may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publisher.

Address permissions requests to: Elsevier Science Rights & Permissions Department, at the mail, fax and e-mail addresses noted above.

Notice

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made.

© The paper used in this publication meets the requirements of ANSI/NISO Z39.48-1992 (Permanence of Paper).

Printed in The Netherlands

Dedication

The idea for a handbook in logic to celebrate the 25th anniversary of the “Studies in Logic” series originated with Einar Fredriksson of North-Holland and the editors of the series. However, between the original idea and the completion of this Handbook, the logic world has been saddened by the deaths of two of the editors — men who were admired as mathematicians and as truly good men by all who knew them. Thus it is only fitting that this book be dedicated to the memories of

ANDRZEJ MOSTOWSKI
and
ABRAHAM ROBINSON.

Foreword

The *Handbook of Mathematical Logic* is an attempt to share with the entire mathematical community some modern developments in logic. We have selected from the wealth of topics available *some* of those which deal with the basic concerns of the subject, or are particularly important for applications to other parts of mathematics, or both.

Mathematical logic is traditionally divided into four parts: model theory, set theory, recursion theory and proof theory. We have followed this division, for lack of a better one, in arranging this book. It made the placement of chapters where there is interaction of several parts of logic a difficult matter, so the division should be taken with a grain of salt. Each of the four parts begins with a short guide to the chapters that follow. The first chapter or two in each part are introductory in scope. More advanced chapters follow, as do chapters on applied or applicable parts of mathematical logic. Each chapter is definitely written for someone who is not a specialist in the field in question. On the other hand, each chapter has its own intended audience which varies from chapter to chapter. In particular, there are some chapters which are not written for the general mathematician, but rather are aimed at logicians in one field by logicians in another.

We hope that many mathematicians will pick up this book out of idle curiosity and leaf through it to get a feeling for what is going on in another part of mathematics. It is hard to imagine a mathematician who could spend ten minutes doing this without wanting to pursue a few chapters, and the introductory sections of others, in some detail. It is an opportunity that hasn't existed before and is the reason for the Handbook.

JON BARWISE

Contributors

- Peter Aczel, *The University of Manchester* (Ch. C.7)
Henk Barendregt, *Mathematisch Instituut, Utrecht* (Ch. D.7)
Jon Barwise, *University of Wisconsin* (Ch. A.1)
John P. Burgess, *Princeton University* (Ch. B.4)
Martin Davis, *Courant Institute, New York University* (Ch. C.2)
Keith J. Devlin, *Lancaster University* (Ch. B.5)
Paul C. Eklof, *University of California, Irvine* (Ch. A.3)
Herbert B. Enderton, *University of California, Los Angeles* (Ch. C.1)
Solomon Feferman, *Stanford University* (Ch. D.4)
Michael P. Fourman, *Mathematics Institute, Oxford* (Ch. D.6)
Leo Harrington, *University of California, Berkeley* (Ch. D.8)
Thomas J. Jech, *Pennsylvania State University* (Ch. B.2)
Istvan Juhász, *Matematikai Kutató Intézet, Budapest* (Ch. B.7)
Alexander Kechris, *California Institute of Technology* (Ch. C.6)
H. J. Keisler, *University of Wisconsin* (Ch. A.2)
A. Kock, *Aarhus University* (Ch. A.8)
Kenneth Kunen, *University of Wisconsin* (Ch. B.3)
Angus Macintyre, *Yale University* (Ch. A.4)
M. Makkai, *McGill University* (Ch. A.7)
Donald A. Martin, *University of California, Los Angeles* (Ch. C.8)
Michael Morley, *Cornell University* (Ch. A.5)
Yiannis N. Moschovakis, *University of California, Los Angeles* (Ch. C.6)
Jeff Paris, *The University of Manchester* (Ch. D.8)
Michael Rabin, *Hebrew University, Jerusalem* (Ch. C.3)
G. E. Reyes, *Université de Montreal* (Ch. A.8)
Mary Ellen Rudin, *University of Wisconsin* (Ch. B.6)
Helmut Schwichtenberg, *Universität Heidelberg* (Ch. D.2)
Richard Shore, *Cornell University* (Ch. C.5)
J. R. Shoenfield, *Duke University* (Ch. B.1)

- Stephen Simpson, *Pennsylvania State University* (Ch. C.4)
C. Smorynski, *State University of New York, Buffalo* (Ch. D.1)
Richard Statman, *University of Michigan* (Ch. D.3)
K. D. Stroyan, *University of Iowa* (Ch. A.6)
A. S. Troelstra, *University of Amsterdam* (Ch. D.5)

Table of Contents

Foreword	vii
Contributors	viii

PART A: MODEL THEORY

Guide to Part A	3
A.1. An introduction to first-order logic, <i>Jon Barwise</i>	5
A.2. Fundamentals of model theory, <i>H. Jerome Keisler</i>	47
A.3. Ultraproducts for algebraists, <i>Paul C. Eklof</i>	105
A.4. Model completeness, <i>Angus Macintyre</i>	139
A.5. Homogenous sets, <i>Michael Morley</i>	181
A.6. Infinitesimal analysis of curves and surfaces, <i>K. D. Stroyan</i>	197
A.7. Admissible sets and infinitary logic, <i>M. Makkai</i>	233
A.8. Doctrines in categorical logic, <i>A. Kock</i> and <i>G. E. Reyes</i>	283

PART B: SET THEORY

Guide to Part B	317
B.1. Axioms of set theory, <i>J.R. Shoenfield</i>	321
B.2. About the axiom of choice, <i>Thomas J. Jech</i>	345
B.3. Combinatorics, <i>Kenneth Kunen</i>	371
B.4. Forcing, <i>John P. Burgess</i>	403
B.5. Constructibility, <i>Keith J. Devlin</i>	453
B.6. Martin's Axiom, <i>Mary Ellen Rudin</i>	491
B.7. Consistency results in topology, <i>I. Juhász</i>	503

PART C: RECURSION THEORY

Guide to Part C.	525
C.1. Elements of recursion theory, <i>Herbert B. Enderton</i>	527
C.2. Unsolvability problems, <i>Martin Davis</i>	567
C.3. Decidable theories, <i>Michael O. Rabin</i>	595
C.4. Degrees of unsolvability: a survey of results, <i>Stephen G. Simpson</i>	631
C.5. α -recursion theory, <i>Richard A. Shore</i>	653
C.6. Recursion in higher types, <i>Alexander Kechris and Yiannis N. Moschovakis</i>	681
C.7. An introduction to inductive definitions, <i>Peter Áczel</i>	739
C.8. Descriptive set theory: Projective sets, <i>Donald A. Martin</i>	783

PART D: PROOF THEORY AND CONSTRUCTIVE MATHEMATICS

Guide to Part D.	819
D.1. The incompleteness theorems, <i>C. Smoryński</i>	821
D.2. Proof theory: Some applications of cut-elimination, <i>Helmut Schwichtenberg</i>	867
D.3. Herbrand's Theorem and Gentzen's notion of a direct proof, <i>Richard Statman</i>	897
D.4. Theories of finite type related to mathematical practice, <i>Solomon Feferman</i>	913
D.5. Aspects of constructive mathematics, <i>A. S. Troelstra</i>	973
D.6. The logic of topoi, <i>Michael P. Fourman</i>	1053
D.7. The type free lambda calculus, <i>Henk Barendregt</i>	1091
D.8. A mathematical incompleteness in Peano Arithmetic, <i>Jeff Paris and Leo Harrington</i>	1133
Author Index	1143
Subject Index	1151

PART A

Model Theory

Guide to Part A: *Model Theory*

with the cooperation of
H. J. KEISLER

A.1. BARWISE	
<i>An introduction to first-order logic</i>	5
A.2. KEISLER	
<i>Fundamentals of model theory</i>	47
A.3. EKLOF	
<i>Ultraproducts for algebraists</i>	105
A.4. MACINTYRE	
<i>Model completeness</i>	139
A.5. MORLEY	
<i>Homogenous sets</i>	181
A.6. STROYAN	
<i>Infinitesimal analysis of curves and surfaces</i>	197
A.7. MAKKAÏ	
<i>Admissible sets and infinitary logic</i>	233
A.8. KOCK and REYES	
<i>Doctrines in categorical logic</i>	283

This part of the Handbook is concerned with the fundamental relationship between mathematical statements (axioms), on the one hand, and mathematical structures (models) which satisfy them, on the other. The emphasis is on the model theory of *first-order* statements. Barwise's chapter, written for those with no prior knowledge of first-order logic, explains the most basic notions. This material is really pre-model theory and is needed for most of the chapters in the Handbook.

Keisler's chapter contains the real introduction to model theory. By glancing through this chapter the reader can see the concerns of the subject illustrated with basic results and applications. The next three chapters treat important topics from model theory in depth and are aimed more at the algebraist.

Eklof's chapter discusses the ultraproduct operation, its relation with first-order logic, and its positive applications to algebra. Macintyre's chapter discusses both positive and negative applications to algebra of Abraham Robinson's notion of *model complete theory* and related concepts of "algebraically closed".

Morley's chapter on homogenous sets discusses so-called Ehrenfeucht–Mostowski models. This construction has proven extremely useful in model theory and in applications to set theory. It has had some applications to other parts of mathematics, but should have more once it becomes better known.

To date the principal application of model theory outside algebra and set theory comes from Robinson's "nonstandard analysis". Stroyan's chapter discusses elementary aspects of the subject and gives a more advanced case study of the hidden role infinitesimals play in differential geometry.

The last three chapters in Part A go beyond ordinary first-order logic. Some extensions of first-order logic are mentioned in the last section of Barwise's chapter and discussed in more detail in the last section of Keisler's chapter. Of all the known extensions, the logic $L_{\omega_1\omega}$ has the smoothest model theory. This logic, and its admissible fragments, are discussed in Makkai's chapter.

The final chapter, by Kock and Reyes, is quite different in character. It gives the category theoretical point of view of some topics from model theory and other parts of logic.

It was planned to have a chapter on stability theory and one on abstract model theory. This proved impossible so stability theory is now surveyed in Section 8 of Keisler's chapter. Abstract model theory is discussed at the end of Barwise's chapter and is touched on in Keisler's chapter. Among the other chapters of the Handbook which are particularly relevant to model theory are Rabin's chapter on decidable and undecidable theories, and Aczel's chapter on inductive definitions, both in Part C of the book.

A.1

An Introduction to First-Order Logic

JON BARWISE*

Contents

1. Foreword	6
2. How to tell if you are in the realm of first-order logic	6
3. The formalization of first-order logic	17
4. The Completeness Theorem	22
5. Beyond first-order logic	41
References	45

* We would like to express our gratitude to the Alfred P Sloan Foundation and the National Science Foundation (MPS 74-06355A1) for support.

1. Foreword

This introductory chapter is written for the (less than ideal) mathematician who knows next to nothing about mathematical logic, and is entirely expository in nature. This might be someone who tried to read a later chapter but got bogged down simply because he did not understand the basic notions. For most readers a quick reading of Section 2 and the introductions to Sections 4 and 5 should suffice.

Modern mathematics might be described as the science of abstract objects, be they real numbers, functions, surfaces, algebraic structures or whatever. Mathematical logic adds a new dimension to this science by paying attention to the language used in mathematics, to the ways abstract objects are defined, and to the laws of logic which govern us as we reason about these objects. The logician undertakes this study with the hope of understanding the phenomena of mathematical experience and eventually contributing to mathematics, both in terms of important results that arise out of the subject itself (Gödel's Second Incompleteness Theorem is the most famous example) and in terms of applications to other branches of mathematics. The chapters of this Handbook are intended to illustrate both of these aspects of mathematical logic.

Modern mathematical logic has its origins in the dream of Leibniz of a universal symbolic calculus which could encompass all mental activity of a logically rigorous nature, in particular, all of mathematics. This vision was too grandiose for Leibniz to realize. His writings on the subject were largely forgotten and had little influence on the actual course of events. It took Boole, Frege, Peano, Russell and Whitehead, Hilbert, Skolem, Gödel, Tarski and their followers, armed with more powerful abstract methods, and motivated (at least in the case of Russell and Hilbert) by apparent problems in the foundations of mathematics, to realize a significant part of Leibniz' dream.

2. How to tell if you are in the realm of first-order logic

Our goal in this section is quite modest: to give the reader, by means of examples, a feeling for what can and what cannot be expressed in first-order logic. Most of our examples are taken from the wealth of notions in modern algebra with which most mathematicians have at least a nodding acquaintance

The basic building blocks of first-order logic consist of the logical

connectives: $\wedge$ (and), $\vee$ (or), $\neg$ (not), $\rightarrow$ (implies), the equality symbol $=$, quantifiers $\forall$ (for all), $\exists$ (there exists) plus an infinite sequence of variables $x, y, z, x_1, y_1, \dots$ and some parentheses $), ($ to help the formulas stay readable.

In addition to these logical symbols, a set L of primitive non-logical symbols is given by the topic under discussion. For example, if we are working with abelian groups then the set L has a function symbol $+$ for group addition and a constant symbol 0 for the zero element. If we are working with orderings, then L has a relation symbol $<$. For the study of set theory, L has a relation symbol $\in$. We will postpone the rather tedious formal definition of formula of first-order logic until the next section. Here we stress only that formulas are certain *finite* strings of symbols.

The “first” in the phrase “first-order logic” is there to distinguish this form of logic from stronger logics (like second-order or weak second-order logic) where certain extralogical notions (like set or natural number) are taken as given in advance. In particular, in first-order logic the quantifiers $\forall$ and $\exists$ always range over elements of the domain M of discourse. By contrast, second-order logic allows one to quantify over subsets of M and functions F mapping, say, $M \times M$ into M . (Third-order logic goes on to sets of functions, etc.) Weak second-order logic allows quantification over finite subsets of M and over natural numbers. There are good reasons for considering first-order logic to be the basic language of mathematics; these will be discussed in Section 5. We assume here that the reader has his own motivation for wanting to find out what first-order logic is.

Group theory

Our first few examples come from group theory. Consider the following notions:

- (a) group,
- (b) abelian group,
- (c) abelian group with every element of order $\leq n$,
- (d) divisible group,
- (e) torsion-free group,
- (f) torsion group.

The notions (a)–(c) are easily axiomatized by a few first-order axioms. Notions (d) and (e) take an infinite list of axioms. The last notion (f) is not first-order. Let’s see why.

A group G is a triple $G = \langle G, +, 0 \rangle$ (where G is a nonempty set, $0 \in G$ and $+$ is a function mapping $G \times G$ into G) which satisfies the following first-order axioms, or sentences:

$$\forall x \forall y \forall z [x + (y + z) = (x + y) + z], \quad (1)$$

$$\forall x [x + 0 = x], \quad (2)$$

$$\forall x \exists y [x + y = 0]. \quad (3)$$

The logician might say that G is a *model* of (1), (2), (3) and write $G \models (1), (2), (3)$, instead of saying that G satisfies (1), (2), (3).

An *abelian group* is a group G satisfying the axiom

$$\forall x \forall y [x + y = y + x]. \quad (4)$$

The choice of the symbol “+” in (1)–(4) is dictated by convention only; it has no real significance.

To express the next notion we abbreviate the formal term $(x + x)$ by $2x$, the term $((x + x) + x)$ by $3x$ and, by induction, we abbreviate the term $(nx + x)$ by $(n + 1)x$. An abelian group G has every element of order $\leq n$ if G is a model of

$$\forall x [x = 0 \vee 2x = 0 \vee \cdots \vee nx = 0]. \quad (5)$$

This is a simple first-order sentence.

An abelian group G is *divisible* if

$$\forall n \geq 1 \forall x \exists y [ny = x]. \quad (6)$$

This would count as a sentence of weak second-order logic but it is *not* a first-order axiom because the leading quantifier ranges over the set of positive natural numbers, rather than over the domain of discourse G . We can, however, replace this expression by the following infinite list of axioms:

$$\forall x \exists y [2y = x], \quad (6)_2$$

$$\forall x \exists y [3y = x], \quad (6)_3$$

$$\vdots$$

$$\forall x \exists y [ny = x], \quad (6)_n$$

$$\vdots$$

(We left off $(6)_1$ since it is the trivial sentence $\forall x \exists y [x = y]$.) For most purposes such an effectively presented infinite list of axioms is practically as good as a finite list. Still, it is worth proving for our own satisfaction that it is not just lack of imagination which forces us to use an infinite list to express the notion.

2.1. PROPOSITION. *Any finite set of first-order sentences true in all divisible abelian groups is true in some nondivisible abelian group.*

In other words, the notion of divisible abelian group is not *finitely* axiomatizable in first-order logic. We delay the proof of this result for a few paragraphs.

We discover essentially the same phenomenon when we attempt to axiomatize the concept of *torsion-free* abelian group:

$$\forall n \geq 1 \forall x [x \neq 0 \rightarrow nx \neq 0]. \quad (7)$$

This sentence of weak second-order logic turns into an infinite list of first-order axioms:

$$\forall x [x \neq 0 \rightarrow nx \neq 0]. \quad (7)_n$$

We have the corresponding negative result.

2.2. PROPOSITION. *The notion of torsion-free abelian group is not finitely axiomatizable in first-order logic.*

An abelian group G is *torsion* if it satisfies

$$\forall x \exists n \geq 1 [nx = 0]. \quad (8)$$

This is a sentence of weak second-order logic but it is not first-order because it has the quantifier $\exists n$ over natural numbers. We could try to imitate (5) but look what happens:

$$\forall x [x = 0 \vee 2x = 0 \vee \cdots \vee nx = 0 \vee \cdots]. \quad (8)'$$

This sort of expression is analogous to an infinite formal power series and the study of such idealized “infinitary formulas” has turned out to be quite profitable (see 5.3, and Chapters A.2 and A.7) but it is not part of ordinary first-order logic. To clinch matters we will prove the following result.

2.3. PROPOSITION. *The set of first-order sentences true in all torsion abelian groups is true in some abelian group H which is not torsion.*

In fact, what we will show is that if G is an abelian group with no finite bound on the order of its elements, then there is a group H which is not torsion but such that $G \equiv H$, which means that every first-order sentence true in G is also true in H , and vice versa. Therefore the class of torsion groups cannot be characterized even by a set of first-order axioms — finite or infinite.

Nonaxiomatizability results

There are two standard tools for proving nonaxiomatizability results. They are corollaries of the Completeness Theorem and will be proved in Section 4. We will use these tools to prove all the results of this section.

2.4. COMPACTNESS THEOREM (Gödel–Malcev). *Let T be any set of first-order axioms. If for every finite subset T_0 of T there is a model of all the axioms in T_0 , then there is a single model of all the axioms in T .*

An alternate form of the Compactness Theorem is sometimes more convenient. Let us write $T \models \psi$ to indicate that ψ is a *logical consequence* of T in the sense that ψ is true in all models which make all the axioms of T true. Then the Compactness Theorem is equivalent to the statement: *If $T \cup \{\psi\}$ is a set of first order sentences and $T \models \psi$, then there is a finite $T_0 \subseteq T$ such that $T_0 \models \psi$.* To see that this follows from 2.4, apply to 2.4 to $T \cup \{\neg\psi\}$, where $\neg\psi$ asserts that ψ is false. To prove 2.4 from this version, let ψ be some absurd ψ like $\exists x (x \neq x)$. The Compactness Theorem *fails* for second-order logic or even weak second-order logic, as the proof of 2.1 will show.

The other property of first-order logic sometimes used to prove nonaxiomatizability results is the following Löwenheim–Skolem Theorem. This important principle also holds for weak second-order logic but not for second-order logic.

2.5. LÖWENHEIM–SKOLEM THEOREM. *Let κ be an infinite cardinal and let T be a set of at most κ first-order axioms. If there is a model making all the axioms in T true, then there is such a model whose set of elements has cardinality $\leq \kappa$.*

Remark. As long as the set L of nonlogical symbols is finite, or even countable, as has been the case up to now, there can be only a countable set of first-order formulas, since every formula is a finite string. Thus, for such L , every set T of axioms which has a model has a *countable* model, by 2.5.

PROOF OF 2.1. Let $\{\psi_1, \dots, \psi_k\}$ be a finite set of first-order sentences true in all divisible abelian groups and let ψ be the conjunction $(\psi_1 \wedge \dots \wedge \psi_k)$. Our task is to prove that ψ is true in some nondivisible abelian group. We apply the second version of the Compactness Theorem. Let T be the set of axioms (1)–(4) plus all the axioms (6)_n. Thus T is a set of axioms for divisible abelian groups. The hypothesis is that $T \models \psi$. By the Compactness

Theorem there is a finite $T_0 \subseteq T$ such that $T_0 \models \psi$. This means that there is an N such that ψ is true in all abelian groups which satisfy $\forall x \exists y [ny = x]$ for $n = 2, \dots, N$. (This much of the proof is common to many proofs.) Taking the first example which comes to mind, let $\mathbb{Z}_p$ be the group of integers mod p , for some prime $p > N$. The group $\mathbb{Z}_p$ is a model of $\forall x \exists y [ny = x]$ for $n < p$, since the map which sends x to nx is one-one and hence onto. Thus ψ is true in $\mathbb{Z}_p$. But $\mathbb{Z}_p$ is far from being divisible since $px = 0$ for all $x \in \mathbb{Z}_p$. $\square$

The proof of 2.2 is just like the proof of 2.1 in form so is left to the reader.

PROOF OF 2.3. Let $G = \langle G, +, 0 \rangle$ be any (possibly torsion) group such that, for each n , there is an element x_n of G of order $\geq n$. For example, G might be the direct sum of all $\mathbb{Z}_p$ over all primes p . We will prove that there is a nontorsion group H such that G and H satisfy exactly the same first-order sentences. Again we use the Compactness Theorem, this time the first version. Take a new constant symbol c and let T consist of all sentences (not mentioning c) true in the group $\langle G, +, 0 \rangle$ plus all the sentences: $2c \neq 0, 3c \neq 0, 4c \neq 0$, etc. Thus T is a set of sentences in a language which has a name c for a new distinguished element. If $H = \langle H, +, 0, c \rangle$ satisfies all the axioms in T then $\langle H, +, 0 \rangle$ will be a group with the same first order axioms true as are true in G but H will not be torsion since the distinguished element c will have infinite order. All we need to see is that there is an H which is a model of all of T . By the Compactness Theorem, it suffices to find a model of each finite $T_0 \subseteq T$. But this is easy. Given T_0 , let N be bigger than all n such that the sentence $nc \neq 0$ is in T_0 . Then we can use x_N to make T_0 true. That is, T_0 is true in the group $\langle G, +, 0, x_N \rangle$ with distinguished element x_N , since the order of x_N is $\geq N$. $\square$

The real numbers

Our first set of examples had to do with whole classes of structures. We now turn to one specific structure, the ordered field $\mathbb{R} = \langle \mathbb{R}, +, \cdot, <, 0, 1 \rangle$ of real numbers. Most students of advanced calculus suffer through a construction of $\mathbb{R}$ and a proof that certain axioms characterize $\mathbb{R}$ up to isomorphism. The axioms are not first-order, however.

2.6. PROPOSITION. *There is no first-order set of axioms which characterize $\mathbb{R}$ up to isomorphism.*

PROOF. By the remark following 2.5, the set of all sentences true in $\mathbb{R}$ is countable. By the Löwenheim–Skolem Theorem, this set has a countable model. $\square$

Since the Löwenheim–Skolem Theorem also holds for weak second-order logic, the proof of 2.6 shows that there is a countable field with the same weak second-order properties as $\mathbb{R}$, among which is the Archimedean axiom:

$$\forall x \exists n [x \leq n1],$$

where $n1$ is the term $((1 + 1) + \cdots + 1)$, n -times, as before. This is a weak second-order statement since the quantifier $\exists n$ ranges not over the elements of an arbitrary model but over the real natural numbers.

The proof of 2.6 is misleading because it makes one feel that the problem has to do with the fact that there are undefinable real numbers, since there are more reals than there are possible definitions in first-order logic with countably many symbols. We can correct this impression by proving a similar result for the enriched structure $\langle \mathbb{R}, +, \cdot, <, r \rangle_{r \in \mathbb{R}}$ where *every* real number r is treated as a distinguished element and is given a name (i.e. constant symbol). We continue the (slightly confusing) practice of using an object r for its own name.

2.7. PROPOSITION. *There is a non-Archimedean field ${}^*\mathbb{R}$ extending $\mathbb{R}$ which satisfies all the first-order sentences true in $\mathbb{R}$, even if we allow names for all real numbers.*

PROOF. The proof is similar, but actually simpler than, the proof of 2.3. We take another new constant symbol c and write the sentence

$$c > r$$

for all real numbers r . To these sentences we add all true first-order sentences of $\mathbb{R}$. By the Compactness Theorem this set of sentences has a model ${}^*\mathbb{R}$. We can consider $\mathbb{R}$ as a submodel of ${}^*\mathbb{R}$. Since the field axioms are true in $\mathbb{R}$ they are also true in ${}^*\mathbb{R}$. $\square$

Most of the theorems of calculus are first-order so that they will hold in ${}^*\mathbb{R}$. Thus 2.5, far from being a negative result, is actually the basis of analysis by means of infinitesimals, or, in other words, Robinson's "nonstandard" analysis. (The element $1/c$ will be a positive infinitesimal.) Thus, it is only a mild exaggeration to say that the universal symbolic calculus of Leibniz' imagination eventually led to a justification of his use

of infinitesimals in the calculus. For more on this, see Chapter A.6 and its 1.1 in particular.

Proposition 2.7 leaves us with the question: Which of the usual axioms for the real numbers is not first-order? The answer is: the completeness axiom,

$$\forall X \subseteq \mathbb{R} [\text{if } X \neq \emptyset \text{ is bounded, then } X \text{ has a l.u.b.}].$$

This is not first-order because the universal quantifier ranges over the set of all subsets X of $\mathbb{R}$. Thus, the proof that the real numbers are unique is really *relative* to a universe of set theory.

Rings and fields

The completeness property of the field of real numbers is not first-order, as we have seen. Let us conclude this introduction into first-order properties by seeing some of the properties of rings and fields that *are* first order. In this discussion our basic language (or vocabulary) L has the nonlogical symbols $+$, $\cdot$, 0 , 1 . The basic axioms for *commutative rings* with identity consist of (1)–(4) above (the abelian group axioms) plus the following first-order axioms:

$$\forall x \forall y [x \cdot y = y \cdot x],$$

$$\forall x \forall y \forall z [(x \cdot y) \cdot z = x \cdot (y \cdot z)],$$

$$\forall x \forall y \forall z [x \cdot (y + z) = (x \cdot y) + (x \cdot z)],$$

$$\forall x [x \cdot 1 = x],$$

$$0 \neq 1.$$

A ring $\mathfrak{R} = \langle R, +, \cdot, 0, 1 \rangle$ is an *integral domain* if it is a model of

$$\forall x \forall y [x \cdot y = 0 \rightarrow (x = 0 \vee y = 0)].$$

Before going on to fields, let us pause to see what to do about a prime concern in ring theory, the notion of an ideal. A proper *ideal* of a commutative ring $\mathfrak{R} = \langle R, +, \cdot, 0, 1 \rangle$ is simply a nonempty, proper subset $I \subseteq R$ which is a subgroup of $\mathfrak{R}$ under addition such that for all $x \in R$ and all $y \in I$, $x \cdot y \in I$. To express this in first-order logic we add a name for I and consider structures of the form $(\mathfrak{R}, I) =_{\text{df}} \langle R, +, \cdot, 0, 1, I \rangle$. Then I is an ideal of $\mathfrak{R}$ if $(\mathfrak{R}, I)$ is a model of the following three axioms. To keep set theory out of the picture, we think of I as a 1-place relation and write $I(x)$ rather than $x \in I$. The middle two axioms assert that I is a subgroup under $+$; the last asserts that I is closed under multiplication by any element x of $\mathfrak{R}$.

$$\begin{aligned}
& I(0) \wedge \neg I(1), \\
& \forall x \forall y [I(x) \wedge I(y) \rightarrow I(x + y)], \\
& \forall x \forall y [I(x) \wedge x + y = 0 \rightarrow I(y)], \\
& \forall x \forall y [I(y) \rightarrow I(x \cdot y)].
\end{aligned}$$

An ideal I is a *prime ideal* if $(\mathfrak{R}, I)$ is a model of

$$\forall x \forall y [I(x \cdot y) \rightarrow I(x) \vee I(y)].$$

Up till now everything has been simple. Either the natural definition of a notion was first-order, or else we have been able to show that the notion is not first-order. This is not always the case. Indeed, some of the most useful applications of logical tools (like ultraproducts) hinge on finding some first-order equivalent to a notion that doesn't look first-order. This is often a nontrivial matter but we give only a simple example. Others can be found in Chapters A.3 and A.4.

An ideal I is a *maximal ideal* of $\mathfrak{R}$ if $(\mathfrak{R}, I)$ is a model of

$$\forall J [I \subseteq J \wedge J \text{ an ideal} \rightarrow J = I \text{ or } J = R]. \quad (9)$$

This is the same form of second-order sentence as the completeness axiom for the reals, but this time we can find an equivalent first-order axiom by recalling the lemma which says that I is maximal in $\mathfrak{R}$ iff the quotient ring $\mathfrak{R}/I$ is a field. To say that $\mathfrak{R}/I$ is a field is to say that for all x , if $x + I$ is not the coset $0 + I$, then there is a y such that $(x + I)(y + I) = 1 + I$. Since $(x + I) \cdot (y + I) = x \cdot y + I$, we can express (9) by the axiom

$$\forall x [\neg I(x) \rightarrow \exists y (x \cdot y + I = 1 + I)]$$

which, when written out in detail becomes

$$\forall x [\neg I(x) \rightarrow \exists y \exists z (I(z) \wedge xy + z = 1)]. \quad (9')$$

While (9)' looses the intuitive content of (9), it is equivalent to (9) and it is first-order, which is what matters here.

Here is a good exercise. A ring $\mathfrak{R}$ is a *principal ideal ring* if $\mathfrak{R}$ is a model of the second-order sentence

$$\forall I [I \text{ an ideal} \rightarrow \exists x \forall y (I(y) \leftrightarrow \exists z (y = zx))].$$

This has the same general form as (9) but it cannot be expressed in first-order logic. Indeed, a simple compactness argument shows that there is a ring $\mathfrak{R}$ with the same first order properties as the ring $\mathbb{Z}$ of integers (written $\mathfrak{R} \equiv \mathbb{Z}$) but where $\mathfrak{R}$ is not a principal ideal ring.

A commutative ring $\mathfrak{N}$ is a *field* if $\mathfrak{N}$ is a model of

$$\forall x \exists y [x \neq 0 \rightarrow x \cdot y = 1].$$

A field R is of *characteristic* p (p a prime) if R is a model of

$$p1 = 0.$$

On the other hand R is of *characteristic* 0 if

$$\forall p [p \text{ a prime} \rightarrow p1 \neq 0]. \quad (10)$$

Did you catch the weak second-order sentence? The quantifier ranges not over $\mathfrak{N}$ but over the prime numbers. Thus we must replace (10) by an infinite list:

$$p1 \neq 0, \quad (10)_p$$

one axiom for each prime p . The result corresponding to Propositions 2.1 and 2.2 becomes more interesting here. The proof is just like the proof of 2.1.

2.8. PROPOSITION. *Any first-order sentence ψ true in all fields of characteristic 0 is true in all fields of characteristic p for sufficiently large p , that is, for p greater than some integer N_ψ .*

Let us abbreviate the formal term $(x \cdot x)$ by x^2 and, by induction, abbreviate the formal term $(x^n \cdot x)$ by x^{n+1} . A field R is *algebraically closed* if it is a model of all axioms of the form

$$\forall x_0 \cdots \forall x_n [x_n \neq 0 \rightarrow \exists y (x_n \cdot y^n + x_{n-1}y^{n-1} + \cdots + x_1y + x_0 = 0)],$$

which says that every polynomial of degree n has a root.

Set theory

The first-order axioms for set theory, are discussed at length in Shoenfield. The basic language L of set theory has only a membership symbol $\in$. The axioms are arrived at by a careful analysis of our informal concept of forming sets, sets of sets, sets of sets of sets, and so on into the transfinite. The resulting set of axioms is called ZF, after Zermelo and Fraenkel. The first axiom about sets one thinks of is the axiom of extensionality: a set is completely determined by its members. This becomes

$$\forall x \forall y [\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y].$$

Properties of mathematical theories

The various first-order theories we have discussed above have radically different properties from a logical point of view. Let us mention a few of them.

The theory of abelian groups is a *decidable theory*, whereas the theory of groups is undecidable. That is, one can give an effective procedure which will tell of an arbitrary sentence ψ involving $+$ and 0 whether or not ψ is a logical consequence of (1)–(4), i.e., whether or not ψ is true in all abelian groups. There can be no such procedure for the theory of groups. This sort of question is dealt with in Chapter C.1 and, more fully, in Chapter C.3.

The theory of algebraically closed fields of a fixed characteristic is a *complete theory*, which is to say that any two algebraically closed fields F_1, F_2 of the same characteristic have all the same first-order properties, i.e., $F_1 \equiv F_2$. On the other hand, most of the first-order theories are not complete. For example, to the theory of rings we can add either $\forall x \exists y [x \neq 0 \rightarrow x \cdot y = 1]$ or its negation $\neg \forall x \exists y [x \neq 0 \rightarrow x \cdot y = 1]$ and have a *consistent theory*. This just amounts to the triviality that some rings are fields and some are not. Combining the above mentioned completeness of the theory of algebraically closed fields with the Completeness Theorem shows, by Theorem 7.2 in Chapter C.1, that the theory of algebraically closed fields of characteristic 0 is *decidable*. Consider the effective procedure P for deciding whether or not a sentence involving $+, \cdot, 0, 1$ is a consequence of this theory. Since all models of this theory have the same first-order properties, we can apply P to decide which sentences involving $+, \cdot, 0, 1$ are true in the field $\mathbb{C} = \langle \mathbb{C}, +, \cdot, 0, 1 \rangle$ of complex numbers. This is expressed by saying that the field $\mathbb{C}$ of complex numbers is a *decidable model*.

Gödel's famous Incompleteness Theorem shows that the ring $\mathbb{Z}$ of integers is *not decidable*. Thus, any mechanical procedure which attempts to decide of sentences ψ involving $+, \cdot, 0, 1$ whether or not ψ is true in $\mathbb{Z}$ must fail for infinitely many sentences. A consequence of this is that any effective list T of true axioms we write down about $\mathbb{Z}$ must inevitably yield an incomplete theory (since otherwise the argument used on $\mathbb{C}$ would work on $\mathbb{Z}$). Gödel's Second Incompleteness Theorem in fact tells us how to go about finding a sentence ψ true in $\mathbb{Z}$ but not a consequence of T . Chapter D.1 contains a thorough discussion of Gödel's Incompleteness Theorems. These results are usually stated in terms of the structure $\mathbb{N} = \langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ of natural numbers, rather than in terms of the ring $\mathbb{Z}$. The standard definition of $\mathbb{Z}$ from $\mathbb{N}$ shows that the results apply equally to $\mathbb{Z}$.

There are a number of topics that could be gone into at this point, but it is more reasonable to let the topics speak for themselves in the chapters that follow. Chapter A.2 discusses the basics of the theory of models for first-order logic. Chapter A.3 treats the ultraproduct construction, an algebraic version of the compactness theorem. Chapter A.4 will also be of particular interest to algebraists, treating as it does, model theoretic analogues of the notion of “algebraically closed” and their applications in algebra. The fundamental results of Ax–Kochen and Ersov are discussed in both of the chapters.

3. The formalization of first-order logic

Let L be a given set of function symbols, relation symbols and constant symbols. We make no restriction on the size of the set L , though usually L is finite or countably infinite. Each function symbol $f \in L$ has a positive integer $\#(f)$ assigned to it; if $n = \#(f)$, then f is called an n -ary function symbol. Similarly, each relation symbol $R \in L$ comes with a positive integer $\#(R)$; if $n = \#(R)$ then R is said to be an n -ary relation symbol.

Examples. For the language $L = \{+, 0\}$ appropriate to group theory there are no relation symbols and $\#(f) = 2$. For the language $L = \{\in\}$ of set theory, there are no functions or constant symbols and $\#(\in) = 2$.

Given a language L we have a natural notion of *structure* or *model* for L . A structure $\mathfrak{M}$ assigns a nonempty collection M of objects over which the quantifiers range, and $\mathfrak{M}$ also assigns appropriate interpretations of the basic primitive relation, function and constant symbols of L .

3.1. DEFINITION. A (*set-theoretic*) *structure* for L is a pair $\mathfrak{M} = \langle M, F \rangle$ where M is a nonempty set and F is an operation with domain L such that, writing $x^{\mathfrak{M}}$ for $F(x)$,

- (i) if $R \in L$ is an n -ary relation symbol, then $R^{\mathfrak{M}} \subseteq M^n$;
- (ii) if $f \in L$ is an n -ary function symbol, then $f^{\mathfrak{M}}: M^n \rightarrow M$;
- (iii) if $c \in L$ is a constant symbol then $c^{\mathfrak{M}} \in M$.

One often writes $\mathfrak{M}$ as $\langle M, R^{\mathfrak{M}}, \dots, f^{\mathfrak{M}}, \dots, c^{\mathfrak{M}}, \dots \rangle$. The parenthetical adjective “set-theoretic” in 3.1 is there because one sometimes wants to consider more generous notions of structures where M may be too large to be a set. For example, the natural structure $\mathfrak{M}$ for the language $L = \{\in\}$ of

set theory has domain M the collection V of all sets, which is not itself a set. However, a consequence of the Completeness Theorem is that any set of axioms that has a model in any reasonable sense will have as a model a reasonably small set theoretic structure. We henceforth deal only with set-theoretic structures.

Example. If $L = \{+, 0\}$ is the language appropriate to group theory, then a structure for L has the form $\mathfrak{M} = \langle M, +^M, 0^M \rangle$ where M is a nonempty set, $+^M : M \times M \rightarrow M$ and $0^M \in M$. We usually use G rather than $\mathfrak{M}$ and drop the superscripts.

We now turn to syntactic notions of first-order logic. Recall the basic building blocks $\wedge, \vee, \neg, \rightarrow, =, \forall, \exists, x, y, z, \dots$, (, mentioned early in Section 2. Let L be a fixed language. Any finite sequence, each element of which is one of these basic symbols or an element of L , is called an *expression*. From the set of expressions we want to single out the ones to which we can assign a meaning.

3.2. DEFINITION. The *terms* of L form the smallest set of expressions containing the variables $x, y, z, \dots$, all constant symbols of L (if any) and closed under the formation rule: if $t_1, \dots, t_n$ are terms of L and if $f \in L$ is an n -ary function symbol, then the expression $f(t_1 \cdots t_n)$ is a term of L . A *closed term* is a term in which no variable appears.

If there are no function symbols in L then the formation rule is vacuous so the only terms are variables and the constants of L .

Example. If $L = \{+, 0\}$ then, strictly speaking, the terms are expressions like

$$+(xy), \quad +(0+(x0)).$$

We naturally agree to abbreviate these by the more natural

$$x + y, \quad 0 + (x + 0),$$

respectively, thus moving the symbol $+$ inside and leaving off the outer parentheses if no confusion arises. As in Section 2 we use nx as an abbreviation of $(\cdots((x+x)+x)+\cdots+x)$, n times, for $n \geq 1$. For this language the only closed terms are the expressions built up from 0 and $+$, none of which are very interesting from a group theoretic point of view.

3.3. DEFINITION. An *atomic formula* of L is an expression of either of the two forms:

$$(t_1 = t_2), \quad R(t_1 \dots t_n)$$

where, in the first case, t_1 and t_2 are terms of L . In the second case $R \in L$ is any n -ary relation symbol and $t_1, \dots, t_n$ are terms of L .

Examples. In the language $L = \{+, 0\}$ of group theory there are not any relation symbols, so the only atomic formulas are statements of equalities between terms, expressions like

$$(x + y = z), \quad (x + y = y + x), \quad (x + y) + z = x + (y + z).$$

In the language $L = \{\in\}$ of set theory where all terms are variables, the only atomic formulas are those of the form $(v = w)$ and $\in(vw)$ for variables v, w . We write the latter as $v \in w$.

3.4. DEFINITION. The first-order *formulas* of L form the smallest set of expressions containing the atomic formulas and closed under the following formation rules:

(i) If φ, ψ are formulas so are the expressions

$$\neg\varphi, \quad (\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \rightarrow \psi);$$

(ii) if φ is a formula and v is a variable, then $(\exists v\varphi)$ and $(\forall v\varphi)$ are formulas.

We associate parentheses to the right in strings where the same symbol is repeated. Thus $\varphi \wedge \psi \wedge \theta$ is $(\varphi \wedge (\psi \wedge \theta))$ and $\varphi \rightarrow \psi \rightarrow \theta$ is $(\varphi \rightarrow (\psi \rightarrow \theta))$.

Example. Let $L = \{+, 0\}$. The following are formulas:

$$\begin{aligned} (x + y = 0), \\ (\exists y (x + y = 0)), \\ (\forall x (\exists y (x + y = 0))) \end{aligned}$$

The last is what we wrote more informally as sentence (3) in Section 2. Note that in the first formula both x and y are sort of “floating free”, in the second formula y is “bound up” by $\exists$ and in the last formula both x and y are “bound”. Only the last formula makes any intuitive sense as an axiom. This is similar to the situation in elementary calculus where

$$x^2 + 2x + 1$$

is an expression which has a variable in it, but the expression

$$\int_0^1 (x^2 + 2x + 1) dx$$

has x “bound”; it has a meaning independent of x . The definite integral is performing roughly the same syntactic role that the quantifiers $\exists$ and $\forall$ play in logic. The next definition makes the notion of “free variable” precise. One can think of it as defined by induction on the length of the formula φ .

3.5. DEFINITION. The set $FV(\varphi)$ of *free variables* of a formula φ is defined as follows:

- (i) If φ is an atomic formula, then $FV(\varphi)$ is just the set of variables appearing in the expression φ ,
- (ii) $FV(\neg\varphi) = FV(\varphi)$,
- (iii) $FV(\varphi \wedge \psi) = FV(\varphi \vee \psi) = FV(\varphi \rightarrow \psi) = FV(\varphi) \cup FV(\psi)$,
- (iv) $FV(\exists v \varphi) = FV(\forall v \varphi) = FV(\varphi) - \{v\}$.

It is common practise to use the notation $\varphi(v_1, \dots, v_n)$ to indicate that $FV(\varphi) \subseteq \{v_1, \dots, v_n\}$ without implying that all of $v_1 \cdots v_n$ are actually free in φ . This is similar to the practise in algebra of writing $p(x_1, \dots, x_n)$ for a polynomial p in the variables $x_1, \dots, x_n$ without implying that all of them have nonzero coefficient.

3.6. DEFINITION. A (*first-order*) *sentence* of L is a formula without any free variables.

So far the terms, formulas and sentences of L are simply finite strings of symbols. We must make sure to assign the intended meanings to our logical symbols so that the formulas of Section 2 express what we intend. This is done by defining the *satisfaction relation* $\mathcal{M} \models \varphi$ between structures on the one hand (the left one) and sentences on the other.

Let $\mathcal{M} = \langle M, \dots \rangle$ be a structure for a language L . An *assignment in* $\mathcal{M}$ is a function s with domain the set of variables of L and range a subset of M . We think of s as assigning a meaning $s(v)$ to the variable v . We can then define, for each term t of L a function $t^{\mathcal{M}}$ which maps assignments to elements of M .

3.7. DEFINITION Let M be given. For t a term of L define $t^{\mathcal{M}}$ as follows:

- (i) If t is a constant symbol c , then $t^{\mathcal{M}}(s) = c^{\mathcal{M}}$ for all s ;
- (ii) if t is a variable v , then $t^{\mathcal{M}}(s) = s(v)$ for all s ;
- (iii) if t is the term $f(t_1 \cdots t_n)$ then, for all s , define

$$t^{\mathcal{M}}(s) = f^{\mathcal{M}}(t_1^{\mathcal{M}}(s), \dots, t_n^{\mathcal{M}}(s)).$$

In (iii), since each of $t_1, \dots, t_n$ is simpler than t we can assume by induction on (the complexity of) terms that $t_1^{\mathfrak{M}}, \dots, t_n^{\mathfrak{M}}$ are already defined. $f^{\mathfrak{M}}$ is defined since $\mathfrak{M}$ is a structure for L and $f \in L$. The reader should note that if $s_1(v) = s_2(v)$ agree on all variables v appearing in t , then $t^{\mathfrak{M}}(s_1) = t^{\mathfrak{M}}(s_2)$. Thus $t^{\mathfrak{M}}$, as a function, depends on only a finite number of values of its argument s .

Example. Let L be the language of rings and let t be the term, or polynomial,

$$x^2 + 2x + 1.$$

Then $t^{\mathfrak{M}}$, for any ring $\mathfrak{R}$, is the corresponding *polynomial function* from $\mathfrak{R}$ into $\mathfrak{R}$. If $s(x) = a$, then $t^{\mathfrak{M}}(s) = a^2 + 2a + 1$, the operations of $+$ and $\cdot$ being those of the ring $\mathfrak{R}$.

In the following definition we use $s(\frac{a}{v})$ for the assignment s' which agrees with s except that $s'(v) = a$.

3.8. DEFINITION. Let $\mathfrak{M}$ be an L -structure. We define a relation

$$\mathfrak{M} \models \varphi[s],$$

(read: the assignment s satisfies the formula φ in $\mathfrak{M}$) for all assignments s and all formulas φ as follows.

- (i) $\mathfrak{M} \models (t_1 = t_2)[s]$ iff $t_1^{\mathfrak{M}}(s) = t_2^{\mathfrak{M}}(s)$,
- (ii) $\mathfrak{M} \models R(t_1 \cdots t_n)[s]$ iff $(t_1^{\mathfrak{M}}(s), \dots, t_n^{\mathfrak{M}}(s)) \in R^{\mathfrak{M}}$,
- (iii) $\mathfrak{M} \models \neg \varphi[s]$ iff not $\mathfrak{M} \models \varphi[s]$,
- (iv) $\mathfrak{M} \models (\varphi \wedge \psi)[s]$ iff $\mathfrak{M} \models \varphi[s]$ and $\mathfrak{M} \models \psi[s]$,
- (v) $\mathfrak{M} \models (\varphi \vee \psi)[s]$ iff $\mathfrak{M} \models \varphi[s]$ or $\mathfrak{M} \models \psi[s]$ or both,
- (vi) $\mathfrak{M} \models (\varphi \rightarrow \psi)[s]$ iff either not $\mathfrak{M} \models \varphi[s]$ or else $\mathfrak{M} \models \psi[s]$,
- (vii) $\mathfrak{M} \models (\exists v \varphi)[s]$ iff there is an $a \in M$ such that $\mathfrak{M} \models \varphi[s(\frac{a}{v})]$,
- (viii) $\mathfrak{M} \models (\forall v \varphi)[s]$ iff for all $a \in M$, $\mathfrak{M} \models \varphi[s(\frac{a}{v})]$.

There is nothing surprising here. It is just making sure that each of our symbols means what we want it to mean. There is one possibly confusing point, in (i), caused by our using $=$ for both the real equality (on the right-hand side) and the symbol for equality (on the left). Many authors abhor this confusion of use and mention and use something like $\equiv$ or $\approx$ for the symbol.

The reader should observe that the truth or falsity of $\mathfrak{M} \models \varphi[s]$ depends only on the values of $s(v)$ for variables v which are actually free in φ . That is, if $s_1(v) = s_2(v)$ for all v free in φ , then $\mathfrak{M} \models \varphi[s_1]$ iff $\mathfrak{M} \models \varphi[s_2]$. Thus, if φ is $\varphi(v_1 \cdots v_n)$ and $a_1 = s(v_1), \dots, a_n = s(v_n)$, then we may write

$\mathcal{M} \models \varphi[a_1, \dots, a_n]$ for $\mathcal{M} \models \varphi[s]$ without confusion. Also, if φ is a sentence, then the truth or falsity of $\mathcal{M} \models \varphi[s]$ is completely independent of s . Thus we may write $\mathcal{M} \models \varphi$ (read: $\mathcal{M}$ is a model of φ , or $\mathcal{M}$ satisfies φ) if for some (hence every) assignment s , $\mathcal{M} \models \varphi[s]$.

If $\varphi(v)$ is a formula and t is a term then $\varphi(t/v)$ (or, more simply, $\varphi(t)$) denotes the result of replacing all occurrences of the free variable v by the term t throughout. When using this notation we always assume that none of the variables in t occur as bound variables in φ . If they did we could always rename the bound variables. Otherwise we would distort the meaning of $\varphi(t)$. For example, if t is w and $\varphi(v)$ is $\exists w (v \neq w)$, then $\varphi(t)$ should assert $\exists w' (w \neq w')$, not $\exists w (w \neq w)$.

A structure $\mathcal{M}$ is a *model of a set Φ* of sentences if $\mathcal{M} \models \varphi$ for all $\varphi \in \Phi$. Given two structure $\mathcal{M}, \mathcal{N}$ for L , we say that $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent*, and write $\mathcal{M} \equiv \mathcal{N}$, iff for all sentences φ of L , $\mathcal{M} \models \varphi$ iff $\mathcal{N} \models \varphi$. If $\mathcal{M} \equiv \mathcal{N}$ (i.e. $\mathcal{M}$ is isomorphic to $\mathcal{N}$, in the obvious sense) then $\mathcal{M} \equiv \mathcal{N}$. Finally, let $\mathcal{K}$ be a class of structures for a language L . $\mathcal{K}$ is (*finitely*) *axiomatizable* if there is a (finite) set Φ of first-order sentences of L such that, for all structures $\mathcal{M}$, $\mathcal{M} \in \mathcal{K}$ iff $\mathcal{M}$ is a model of Φ . This agrees with our terminology in Section 2. Some authors call a finitely axiomatizable class an *elementary class*, or EC. They are then forced into calling an axiomatizable class *elementary in the wider sense*, or EC_Δ .

4. The Completeness Theorem

Surely the most important discovery for mathematics by the ancient Greeks was of the notion of *proof*, turning mathematics into a deductive science. Each theorem φ must have a proof from a set T of more or less explicitly stated assumptions, or *axioms*. The proof must demonstrate that the conclusion φ follows from the axioms in T by the laws of logic alone. The mathematician implicitly assumes that he understands the notion of proof and that, in particular, he will be able to check in a rigorous manner whether a purported complete proof does indeed establish the conclusion from the stated assumptions. The natural question is: Can the notions “laws of logic” and “proof” be made mathematically precise?

In this section we want to show that there is a mathematically precise notion of “ φ is provable from T ” which captures completely the intuitive notion “ φ follows from T by the laws of logic alone”, for first-order φ and T . More fully, we want to provide a concrete set of obviously valid rules of inference such that φ follows from T by the laws of logic alone if and only

if there is a proof of φ from axioms in T which uses only the permitted rules of inference.

There is a seeming obstacle to our program. How can we hope to prove such a result without knowing in advance what it means to follow by the laws of logic alone? Luckily, we do not need to know. All we need is to agree that, whatever it means, it at least *implies* that φ will hold in all set theoretic structures which are models of T ; i.e., it implies $T \models \varphi$. Thus, to realize our goal, it more than suffices to provide valid rules of inference and show that $T \models \varphi$ if and only if φ is provable from T . This is the content of Gödel's Completeness Theorem.

The plan of this section is as follows. In 4.1 and 4.2 we take care of so-called propositional logic. In 4.3–4.8 we discuss a method, due in essence to Henkin, for reducing certain problems of first-order logic back to problems about propositional logic. The proofs of the Compactness Theorem and the Löwenheim–Skolem Theorem fall out of this method. Finally we present two different versions of the Gödel Completeness Theorem which are consequences of 4.8., a Hilbert-style formal system (4.9) and a Gentzen-style formal system (4.13).

Propositional logic

It is expeditious to break the study of first-order logic up into two parts, the trivial part having to do with the propositional connectives $\wedge, \vee, \neg, \rightarrow$, and then the part having to do with equality and the quantifiers $\forall$ and $\exists$.

Let P be a set of objects called *prime formulas*. They might be sentences of some natural language or letters $p, q, r, \dots$ of the alphabet, for example. In our application, they will be those first-order formulas which are not propositional combinations of simpler formulas, that is, atomic formulas and formulas beginning with a quantifier. The set of *propositional formulas* of P form the smallest set of expressions containing the members of P and closed under the rule: if A, B are propositional formulas then so are $\neg A$, $(A \wedge B)$, $(A \vee B)$ and $(A \rightarrow B)$. The *prime constituents* of a propositional formula A are just the prime formulas out of which A is built.

Examples. Suppose $P = \{p, q, r\}$. The following are propositional formulas of P :

$$p, \quad q, \quad (p \vee q), \quad (q \vee p), \quad ((p \vee q) \rightarrow (q \vee p)).$$

We want to show exactly how the truth or falsity of a propositional formula depends on the truth or falsity of its prime constituents. Then, going a step further, we show how to decide which propositional formulas

are always true, regardless of the truth or falsity of their prime constituents, formulas like $(p \vee \neg p)$, $((p \rightarrow q) \wedge \neg q) \rightarrow \neg p$, etc. Such formulas are called propositional *tautologies*, since they are true by virtue of their syntactic form alone. These tautologies provide a small first step in isolating the laws of logic.

Let **t** and **f** be distinct new symbols, thought of as “true” and “false”. A *truth assignment* for a set P of prime formulas is, by definition, a function $\nu : P \rightarrow \{\mathbf{t}, \mathbf{f}\}$. For each truth assignment ν we define its extension $\bar{\nu}$ to the set of all propositional formulas of P by induction on length of formulas as follows:

$$\begin{aligned}\bar{\nu}(A) &= \nu(A) \quad \text{if } A \text{ is prime;} \\ \bar{\nu}(\neg A) &= \mathbf{f} \quad \text{if } \bar{\nu}(A) = \mathbf{t}, \\ &= \mathbf{t} \quad \text{if } \bar{\nu}(A) = \mathbf{f}; \\ \bar{\nu}(A \wedge B) &= \mathbf{t} \quad \text{if } \bar{\nu}(A) = \bar{\nu}(B) = \mathbf{t}, \\ &= \mathbf{f} \quad \text{otherwise;} \\ \bar{\nu}(A \vee B) &= \mathbf{t} \quad \text{if } \bar{\nu}(A) = \mathbf{t} \text{ or } \bar{\nu}(B) = \mathbf{t} \text{ or both,} \\ &= \mathbf{f} \quad \text{otherwise;} \\ \bar{\nu}(A \rightarrow B) &= \mathbf{f} \quad \text{if } \bar{\nu}(A) = \mathbf{t} \text{ and } \bar{\nu}(B) = \mathbf{f}, \\ &= \mathbf{t} \quad \text{otherwise.}\end{aligned}$$

This definition can be summarized by means of the following *truth table*:

A	B	$\neg A$	$(A \wedge B)$	$(A \vee B)$	$(A \rightarrow B)$
t	t	f	t	t	t
t	f	f	f	t	f
f	t	t	f	t	t
f	f	t	f	f	t

By constructing such truth tables we can completely analyze how the truth or falsity of a propositional formula depends on the truth or falsity of its prime constituents. We illustrate the method for the formula

$$((\neg(p \wedge \neg q) \wedge q) \rightarrow p).$$

We simplify the table by leaving out some of the **t**'s.

p	q	$\neg q$	$p \wedge \neg q$	$\neg(p \wedge \neg q)$	$\neg(p \wedge \neg q) \wedge q$	$(\neg(p \wedge \neg q) \wedge q) \rightarrow p$
t	t	f	f			
t	f			f	f	
f	t	f	f			f
f	f		f		f	

Thus, the only circumstances under which our final formula is false is when p is false and q is true.

4.1. DEFINITION. A propositional formula A of P is a *tautology* if $\bar{\nu}(A) = \mathbf{t}$ for all truth assignments $\nu : P \rightarrow \{\mathbf{t}, \mathbf{f}\}$. A is *consistent* if $\bar{\nu}(A) = \mathbf{t}$ for some $\nu : P \rightarrow \{\mathbf{t}, \mathbf{f}\}$.

The method of truth tables makes it a trivial matter to see whether a propositional formula is a tautology or not, or whether it is consistent or not. If we write $A \leftrightarrow B$ for $(A \rightarrow B) \wedge (B \rightarrow A)$, then we see that the following are tautologies:

$(A \vee \neg A)$ (law of the excluded middle),

$\neg(A \wedge \neg A)$ (law of contradiction),

$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$
 $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$ (de Morgan's laws),

$\neg\neg A \leftrightarrow A$ (law of double negation).

Just to make sure the method of truth tables is perfectly clear, we present an example with three prime constituents p, q, r :

$$\underbrace{[(p \wedge q) \rightarrow r]}_A \wedge \underbrace{(\neg r \rightarrow q)}_B \rightarrow \underbrace{(p \rightarrow r)}_C$$

p	q	r	$p \wedge q$	A	$\neg r$	B	$A \wedge B$	C	$[A \wedge B] \rightarrow C$
t	t	t			f				
t	t	f		f			f	f	
t	f	t	f		f				
t	f	f	f			f	f	f	
f	t	t	f		f				
f	t	f	f						
f	f	t	f		f				
f	f	f	f			f	f		

Thus, since no falses turn up in the last column, the formula is indeed a tautology.

In practise, there is a much shorter method to check to see whether a formula is or is not a tautology. One works backwards, trying to find a consistent assignment which makes the formula false. Applied to the above, to make $[A \wedge B] \rightarrow C$ false, we need to have $\bar{\nu}(A) = \bar{\nu}(B) = \mathbf{t}$ but $\bar{\nu}(C) = \mathbf{f}$. To make $\bar{\nu}(C) = \mathbf{f}$, we must make $\bar{\nu}(p) = \mathbf{t}$, $\bar{\nu}(r) = \mathbf{f}$. To have $\bar{\nu}(B) = \mathbf{t}$ we must have $\bar{\nu}(q) = \mathbf{t}$, since $\bar{\nu}(\neg r) = \mathbf{t}$. But now we have $\bar{\nu}(p) = \bar{\nu}(q) = \mathbf{t}$ and $\bar{\nu}(r) = \mathbf{f}$ which gives $\bar{\nu}(A) = \mathbf{f}$, a contradiction. Thus the above formula is a tautology.

A set T of propositional formulas is said to be *consistent* (in the sense of propositional logic) if there is a truth assignment ν such that $\bar{\nu}(A) = \mathbf{t}$ for all $A \in T$.

4.2. COMPACTNESS THEOREM FOR PROPOSITIONAL LOGIC. *A set T of propositional formulas is consistent if and only if every finite subset of T is consistent.*

PROOF. We present two proofs of the nontrivial half.

First proof. For the purposes of this proof call a set S *finitely consistent* if every finite subset of S is consistent. We wish to prove that every finitely consistent set is consistent. Call S *maximal* finitely consistent if S is finitely consistent and for every formula A , either $A \in S$ or $(\neg A) \in S$.

There is a natural correspondence between valuations ν and maximal, finitely consistent sets. To any ν assign the set $S_\nu = \{A \mid \bar{\nu}(A) = \mathbf{t}\}$. This set is maximal, finitely consistent. Conversely, given a maximal, finitely consistent set S , define $\nu(p) = \mathbf{t}$ if $p \in S$, $\nu(p) = \mathbf{f}$ if $p \notin S$. The following facts follow immediately from the fact that S is maximal, finitely consistent, and imply (by induction on formulas A) that $S = S_\nu$:

$$\begin{aligned} B \in S & \text{ iff } (\neg B) \notin S, \\ (A \wedge B) \in S & \text{ iff } A \in S \text{ and } B \in S, \\ (A \vee B) \in S & \text{ iff } A \in S \text{ or } B \in S, \\ (A \rightarrow B) \in S & \text{ iff } A \notin S \text{ or } B \in S. \end{aligned}$$

For example, let's prove that $(A \vee B) \in S$ implies $A \in S$ or $B \in S$. Suppose not. Then $(A \vee B) \in S$ but $(\neg A) \in S$ and $(\neg B) \in S$, by maximality. But then $\{(A \vee B), \neg A, \neg B\}$ is a finite, inconsistent subset of S , a contradiction.

The above remarks show that proving a finitely consistent set T consistent is equivalent to finding a maximal, finitely consistent set $S \supseteq T$.

We show how to construct such an S in the case where the underlying set P of prime formulas is countable. Essentially the same proof works as long as P is well-ordered and hence, by the axiom of choice, works for all P . The proof for well-ordered P does not need the axiom of choice.

If P is countable, so is the set of all formulas so we enumerate them: $A_1, A_2, \dots, A_n, \dots$. Define $T_0 \subseteq T_1 \subseteq \dots \subseteq T_n \subseteq \dots$ by

$$T_0 = T;$$

$$T_{n+1} = T_n \cup \{A_n\} \quad \text{if this is finitely consistent,}$$

$$= T_n \cup \{\neg A_n\} \quad \text{otherwise.}$$

Let $S = \bigcup T_n$. Clearly $T \subseteq S$ and for every A , either $A \in S$ or $(\neg A) \in S$. To finish the proof we need only show that each T_n , and hence S , is finitely consistent. This is proved by induction on n with $n = 0$ being the hypothesis of the theorem that T is finitely consistent. Assume T_n is finitely consistent, and prove that T_{n+1} is finitely consistent.

Case 1. $T_{n+1} = T_n \cup \{A_n\}$. By the definition of T_{n+1} , this is finitely consistent.

Case 2. $T_{n+1} = T_n \cup \{\neg A_n\}$. This can only happen if there is some finite set $T'_n \subset T_n$ such that $T'_n \cup \{A_n\}$ is not consistent. Suppose that T_{n+1} is not finitely consistent. Then there is a finite set $T''_n \subseteq T_n$ such that $T''_n \cup \{\neg A_n\}$ is not consistent. But then $T'_n \cup T''_n$ is a finite subset of T_n so is consistent. Any assignment ν making all of $T'_n \cup T''_n$ true must make *one* of A_n or $\neg A_n$ true, contradicting the inconsistency of both $T'_n \cup \{A_n\}$ and $T''_n \cup \{\neg A_n\}$.

Thus, in either case, T_{n+1} is after all finitely consistent. This finishes the proof.

Second proof. We can give a faster proof by quoting the Tychonoff Theorem. It hides the basic construction, though, and thus is less suitable for other constructions in model theory. Let $2 = \{\mathbf{t}, \mathbf{f}\}$ be the two elements space with the discrete topology and let $X = 2^P$, the space of all truth assignments of P with the product topology. By the Tychonoff Theorem X is a compact, Hausdorff space. Hence if $\mathcal{F} = \{F_i \mid i \in I\}$ is an indexed family of closed subsets, and if $\bigcap_{i \in I} F_i = \emptyset$, then there is a finite $I_0 \subseteq I$ such that $\bigcap_{i \in I_0} F_i = \emptyset$. For each propositional formula A , let $F_A = \{\nu \in X \mid \bar{\nu}(A) = \mathbf{t}\}$. We claim that each F_A is clopen (both closed and open) in X . For $A = p$ a prime formula F_p is open by the very definition of the product topology. But $X - F_p = \{\nu \mid \nu(p) = \mathbf{f}\}$ is also open, by definition, so F_p is clopen. For more complicated formulas, the claim follows by induction on length of formulas and the following equations:

$$\begin{aligned}
 F_{(A \vee B)} &= F_A \cup F_B, & F_{(A \wedge B)} &= F_A \cap F_B, \\
 F_{(A \rightarrow B)} &= F_B - F_A, & F_{\neg A} &= X - F_A.
 \end{aligned}$$

This establishes the claim. Now let T be as given in the theorem. By hypothesis, for each finite $T_0 \subseteq T$, there is a $\bar{v}$ making all $\varphi \in T_0$ true, i.e. $\bigcap_{A \in T_0} F_A \neq \emptyset$. By the compactness of X , $\bigcap_{A \in T} F_A \neq \emptyset$. Thus, there is a truth assignment $\bar{v}$ making all $A \in T$ true. $\square$

The standard classroom example of a simple application of the Compactness Theorem for Propositional Logic is to prove that if an infinite map cannot be colored by k colors then some finite submap cannot be colored by k colors. To prove this one assigns k prime formulas to each “country” on the map, one for each color, and writes down the obvious “axioms” asserting that each country gets exactly one color “true” and that adjacent countries do not have the same color “true”. Another example, if one gives the first proof of the Compactness Theorem, is to prove the Tychonoff Theorem for 2^P .

The use of Henkin constants for reducing first-order logic to propositional logic

In this subsection we apply the notions of propositional logic to first-order logic. Given a language L let P be the set of formulas of L which are atomic or begin with $\forall$ or $\exists$. Thus, a *tautology of first-order logic* is any formula which is true regardless of what truth assignment is given to the prime formulas. For example the following are tautologies,

$$\begin{aligned}
 &\forall x R(x) \vee \neg \forall x R(x), \\
 &\neg (\forall x R(x) \wedge \exists x S(x)) \leftrightarrow (\neg \forall x R(x) \vee \neg \exists x S(x)),
 \end{aligned}$$

but the following sentences are not tautologies:

$$\begin{aligned}
 &(c = c), \\
 &\forall x (R(x) \vee \neg R(x)), \\
 &\neg \exists x S(x) \rightarrow \forall x \neg S(x).
 \end{aligned}$$

The first two are prime formulas, the third has the form $\neg p \rightarrow q$ for prime p and q . We see that the tautologies of first-order logic barely scratch the surface of the collection of “laws of logic”

We state an obvious lemma for the record.

4.3. LEMMA. Let $\mathfrak{M} = \langle M, \dots \rangle$ be a structure for a language L and let s be an assignment in $\mathfrak{M}$, i.e., a function mapping the variables of L into M . There is a truth assignment ν to the prime formulas of L such that, for all formulas φ of L , $\mathfrak{M} \models \varphi[s]$ if and only if $\bar{\nu}(\varphi) = \mathbf{t}$. In particular, any set of sentences true in $\mathfrak{M}$ is consistent in the sense of propositional logic.

PROOF. For φ a prime formula, define $\nu(\varphi) = \mathbf{t}$ if $\mathfrak{M} \models \varphi[s]$, otherwise $\nu(\varphi) = \mathbf{f}$. Since every formula is built up from prime formulas by means of propositional connectives, the conclusion is obvious. $\square$

The converse of the lemma is far from true. For example the following set of sentences is consistent in the sense of propositional logic (they are all prime formulas) but has no model:

$$\{\forall x (R(x) \rightarrow S(x)), \forall x R(x), \exists x \neg S(x)\}.$$

There has been no analysis of the quantificational structure of the sentences.

4.4. EQUALITY AXIOMS. The equality axioms are as follows, where $u, w, u_1, \dots$ denote variables and constant symbols of L :

$$(u = u),$$

$$(u = w) \rightarrow (w = u),$$

$$(u_1 = u_2 \wedge u_2 = u_3) \rightarrow (u_1 = u_3),$$

$$(u_1 = w_1 \wedge \dots \wedge u_n = w_n) \rightarrow (R(u_1 \dots u_n) \rightarrow R(w_1 \dots w_n)),$$

$$(u_1 = w_1 \wedge \dots \wedge u_n = w_n) \rightarrow (t(u_1 \dots u_n) = t(w_1 \dots w_n)),$$

where R is an arbitrary n -ary relation symbol of L and t is an arbitrary n -ary term of L . The equality axioms are *valid* in that for all such axioms φ , all $\mathfrak{M}$ and all assignments s to variables, $\mathfrak{M} \models \varphi[s]$. The last four axioms for equality might well be called Leibniz Law.

The *witnessing expansion* $L(C)$ of a language L is constructed as follows. Let $C_0 = \emptyset$ and, once C_n is defined, let $L_n = L \cup C_n$. For each formula $\varphi(v)$ of L_0 with exactly one free variable let $c_{\varphi(v)}$ be a distinct new constant symbol and let C_1 be the set of all these $c_{\varphi(v)}$. Given C_n , assign distinct new constant symbols $c_{\varphi(v)}$ to each formula $\varphi(v)$ of L_n which is not already a formula of L_{n-1} (i.e., if some constant from C_n appears in φ). Let C_{n+1} be C_n union the set of all these new $c_{\varphi(v)}$. Let $C = \bigcup_n C_n$ and let $L(C) = L \cup C$.

4.5. DEFINITION. The constant symbol $c_{\varphi(v)}$ is called a *witnessing constant* and the sentences

$$\text{I} \quad (\exists v \varphi(v)) \rightarrow \varphi(c_{\varphi(v)}),$$

$$\text{II} \quad \varphi(c_{\neg\varphi(v)}) \rightarrow \forall v \varphi(v)$$

are called *Henkin axioms* of types I and II.

The informal idea behind the Henkin axioms is quite simple. If $\exists v \varphi(v)$ is true in a structure, choose an element a satisfying $\varphi(v)$ and give it a new name $c_{\varphi(v)}$. If $\forall v \varphi(v)$ is false, choose a counterexample b and call it by the new name $c_{\neg\varphi(v)}$.

4.6. DEFINITION. T_{Henkin} is, by definition, the set of all sentences of $L(C)$ which are either Henkin axioms or else of one of the forms:

$$\text{III} \quad \forall v \varphi(v) \rightarrow \varphi(t), \quad t \text{ a closed term of } L(C);$$

$$\text{IV} \quad \varphi(t) \rightarrow \exists v \varphi(v), \quad t \text{ a closed term of } L(C).$$

These latter are called the *quantifier axioms*. Their informal content is clear.

The set T_{Henkin} is not true in every $L(C)$ -structure, but the next lemma shows that every L -structure can be turned into an $L(C)$ -structure which is a model of T_{Henkin} , using the idea discussed following 4.5.

If $L \subseteq L'$ are languages and $\mathfrak{M}' = \langle M, F' \rangle$ is a structure for L' then $\mathfrak{M} = \langle M, F' \upharpoonright L \rangle$ is called the *reduct* of L' to L and $\mathfrak{M}'$ is called an *expansion* of $\mathfrak{M}$ to the language L' . Thus, $\mathfrak{M}$ and $\mathfrak{M}'$ are the same except that $\mathfrak{M}'$ assigns meanings to the symbols in $L' - L$.

4.7. LEMMA. *Let $\mathfrak{M}$ be any structure for a language L and let $L(C)$ be the witnessing expansion of L . There is an assignment of elements of $\mathfrak{M}$ to the constant symbols of C so that the resulting expansion of $\mathfrak{M}$ is a model of T_{Henkin} .*

PROOF. The quantifier axioms III, IV are going to be true regardless, so we only need worry about those of types I, II. Suppose we contrive to make those of type I true, and consider a typical one of type II:

$$\varphi(c_{\neg\varphi(v)}) \rightarrow \forall v \varphi(v).$$

Suppose the hypothesis is true in the expansion, but not the conclusion.

But then $\exists v \neg \varphi(v)$ is true, so by I, $\neg \varphi(c_{\neg \varphi(v)})$ is true, a contradiction. Thus, if all axioms of type I are true, so are all of type II.

We proceed to assign elements to the constants in C_n by induction on n . If $c_{\varphi(v)} \in C_1$ then $\exists v \varphi(v)$ is a sentence of L and hence makes sense in $\mathfrak{M}$. If $\mathfrak{M} \models \exists v \varphi(v)$, choose some $a \in M$ so that $\mathfrak{M} \models \varphi(a)$ and set $c_{\varphi(v)}^{\mathfrak{M}} = a$. If $\mathfrak{M} \models \neg \exists v \varphi(v)$, define $c_{\varphi(v)}^{\mathfrak{M}}$ arbitrarily. This makes all the positive Henkin axioms about the $c_{\varphi(v)} \in C_1$ true. But once the constants of C_1 are interpreted, all the sentences of $L_1 = L \cup C_1$ make sense, so we can carry out the same argument and assign elements to the $c_{\varphi(v)} \in C_2$, and so on. $\square$

A *canonical structure* for $L(C)$ is a structure $\mathfrak{M} = \langle M, \dots \rangle$ such that every $a \in M$ is denoted by some $c \in C$. That is, $M = \{c^{\mathfrak{M}} \mid c \in C\}$. The set Eq mentioned in 4.8 is the set of equality axioms of $L(C)$ which are sentences of $L(C)$; i.e., those which contain no variables.

The following lemma may seem rather technical but the equivalence of (i) and (iii) show that we have reduced problems about models of first-order theories to essentially trivial questions about propositional logic. There is a price to be paid, however. Even in the case where the T in (i) is finite, the propositional theory in (iii) is infinite.

4.8. MAIN LEMMA (The reduction to propositional logic). *Let L be a first-order language and let $L(C)$ be the witnessing expansion of L . For any set T of sentences of L the following conditions are equivalent:*

- (i) *T has a model; i.e. there is an L -structure $\mathfrak{M}$ which is a model of all sentences in T .*
- (ii) *There is a canonical $L(C)$ -structure $\mathfrak{M}$ which is a model of all sentences in T .*
- (iii) *$T \cup T_{\text{Henkin}} \cup \text{Eq}$ is consistent in the sense of propositional logic.*

PROOF. The implication (ii) $\Rightarrow$ (i) is immediate, while (i) $\Rightarrow$ (iii) follows from Lemma 4.3. We prove (iii) $\Rightarrow$ (ii). Let ν be a truth assignment to the prime sentences of $L(C)$ such that $\nu(\varphi) = \mathbf{t}$ for all $\varphi \in T \cup T_{\text{Henkin}} \cup \text{Eq}$. To prove the lemma, we construct a canonical model $\mathfrak{M} = \langle M, \dots \rangle$ such that, for all sentences φ of $L(C)$,

$$\mathfrak{M} \models \varphi \quad \text{iff} \quad \bar{\nu}(\varphi) = \mathbf{t}.$$

The main function of T_{Henkin} is to guarantee that $\bar{\nu}$ satisfies the following conditions:

$$\bar{\nu}(\exists v \varphi(v)) = \mathbf{t} \quad \text{iff} \quad \bar{\nu}(\varphi(c_{\varphi(v)})) = \mathbf{t},$$

$$\bar{\nu}(\forall v \varphi(v)) = \mathbf{t} \quad \text{iff} \quad \bar{\nu}(\varphi(t)) = \mathbf{t} \quad \text{for all closed terms } t \text{ of } L(C).$$

The conditions allow us to construct our model $\mathfrak{M}$ out of the constants in C in a way that is analogous to the construction of a group from generators (the elements of C) and defining relations (the axioms of T). To define $\mathfrak{M}$ we must (a) specify the universe M of $\mathfrak{M}$, (b) define, for each n -ary relation symbol $R \in L$ an n -ary relation $R^{\mathfrak{M}}$ to interpret R , (c) define for each n -ary function symbol $f \in L$ an interpretation $f^{\mathfrak{M}}: M^n \rightarrow M$, and (d) define for each constant symbol c of $L \cup C$ an element $c^{\mathfrak{M}} \in M$. Having thus constructed $\mathfrak{M}$ it will remain only to verify that $\mathfrak{M} \models \varphi$ iff $\bar{\nu}(\varphi) = \mathbf{t}$, for all sentences φ of $L(C)$. This condition tells us how we must fulfill conditions (b)–(d) above.

(a) Define an equivalence relation $\approx$ on C by

$$c \approx d \quad \text{iff} \quad \nu((c = d)) = \mathbf{t}.$$

The equality axioms guarantee that $\approx$ is an equivalence relation on C . Suppose, for example, that $c \approx d$ and $d \approx e$. We check to see that $c \approx e$. Since $\nu(c = d) = \mathbf{t}$, $\nu(d = e) = \mathbf{t}$ by $c \approx d$, $d \approx e$ and since $\bar{\nu}(((c = d \wedge d = e) \rightarrow c = e)) = \mathbf{t}$ since this sentence is an equality axiom, $\nu(c = e) = \mathbf{t}$ so $c \approx e$. Let $\bar{c}$ be the equivalence class of c and let $M = \{\bar{c} \mid c \in C\}$.

(b) Define $R^{\mathfrak{M}}$ by

$$\langle \bar{c}_1, \dots, \bar{c}_n \rangle \in R^{\mathfrak{M}} \quad \text{iff} \quad \nu(R(c_1, \dots, c_n)) = \mathbf{t}.$$

To see that this is well defined we must check that if

$$\bar{c}_1 = \bar{d}_1, \dots, \bar{c}_n = \bar{d}_n \quad \text{and} \quad \langle \bar{c}_1, \dots, \bar{c}_n \rangle \in R^{\mathfrak{M}},$$

then $\langle \bar{d}_1, \dots, \bar{d}_n \rangle \in R^{\mathfrak{M}}$. This is a consequence of the fact that

$$c_1 = d_1 \wedge \dots \wedge c_n = d_n \wedge R(c_1, \dots, c_n) \rightarrow R(d_1, \dots, d_n)$$

is an equality axiom and hence is assigned true by $\bar{\nu}$.

(c) Let $c_1, \dots, c_n \in C$ and $f \in L$ be given. We claim there is a $c \in C$ such that $\nu(f(c_1 \dots c_n) = c) = \mathbf{t}$. For consider the formula $\varphi(x)$ given by $(f(c_1 \dots c_n) = x)$. If $\bar{\nu}(\exists v \varphi(v)) = \mathbf{t}$, then $\nu(f(c_1 \dots c_n) = c_\varphi) = \mathbf{t}$. So suppose that $\nu(\exists v \varphi(v)) = \mathbf{f}$. But one member of T_{Henkin} is the sentence $(\varphi(f(c_1 \dots c_n)) \rightarrow \exists v \varphi(v))$ so that $\bar{\nu}(\varphi(f(c_1 \dots c_n))) = \mathbf{f}$. But this says that ν assigns $\mathbf{f}$ to the atomic sentence $(f(c_1 \dots c_n) = f(c_1 \dots c_n))$. But $\bar{\nu}(c_i = c_i) = \mathbf{t}$, $(i = 1, \dots, n)$ and $\bar{\nu}((c_1 = c_1 \wedge \dots \wedge c_n = c_n) \rightarrow (f(c_1 \dots c_n) = f(c_1 \dots c_n))) = \mathbf{t}$ since these are equality axioms, which is a contradiction. Thus $\bar{\nu}(\exists v \varphi(v)) = \mathbf{t}$ after all. We can define $f^{\mathfrak{M}}(\bar{c}_1, \dots, \bar{c}_n) = \bar{c}$ for that $c \in C$ such that $\nu(f(c_1 \dots c_n) = c) = \mathbf{t}$. An argument like that used in (b) shows that $f^{\mathfrak{M}}$ is well defined.

(d) If $c \in C$ let $c^{\mathfrak{M}} = \bar{c}$. If $d \in L$, then an argument similar to that used in (c) shows that there is a $c \in C$ such that $\nu(d = c) = \mathbf{t}$ so let $d^{\mathfrak{M}} = \bar{c}$ for this c .

This completes the construction of $\mathfrak{M}$ and guarantees that for atomic sentences $\mathfrak{M} \models \varphi$ iff $\nu(\varphi) = \mathbf{t}$. To prove this for other sentences we proceed by induction on length of formulas. The propositional connectives are trivial. For example, $\mathfrak{M} \models (\varphi \wedge \psi)$ iff $\mathfrak{M} \models \varphi$ and $\mathfrak{M} \models \psi$ (by definition of $\models$) iff $\bar{\nu}(\varphi) = \bar{\nu}(\psi) = \mathbf{t}$ (by the induction hypothesis) iff $\bar{\nu}(\varphi \wedge \psi) = \mathbf{t}$. Suppose φ is $\exists x \psi(x)$. If $\bar{\nu}(\varphi) = \mathbf{t}$ then, by the condition above, there is a c such that $\bar{\nu}(\varphi(c)) = \mathbf{t}$ so, by induction hypothesis, $\mathfrak{M} \models \psi(c)$ so $\mathfrak{M} \models \exists x \psi(x)$ so $\mathfrak{M} \models \varphi$. On the other hand, if $\bar{\nu}(\varphi) = \mathbf{f}$ then $\bar{\nu}(\exists x \psi(x)) = \mathbf{f}$ so by T_{Henkin} , $\bar{\nu}(\psi(t)) = \mathbf{f}$ for all closed terms t of $L(C)$. In particular, for every $c \in C$, $\bar{\nu}(\psi(c)) = \mathbf{f}$. By the induction hypothesis, $\mathfrak{M} \models \neg \psi(c)$ for all $c \in C$. Since every element of M is denoted by some $c \in C$, $\mathfrak{M} \models \neg \exists x \psi(x)$. Thus $\mathfrak{M} \models \exists x \psi(x)$ iff $\nu(\exists x \psi(x)) = \mathbf{t}$. The proof in the case when φ begins with $\forall$ is similar. $\square$

The Main Lemma provides a method for actually constructing models of theories out of symbols. In particular, it gives us immediate proofs of the Compactness and Lowenheim–Skolem Theorems.

PROOF OF THE COMPACTNESS THEOREM (2.4). Let T be a set of sentences of the first-order language L such that every finite subset of T has a model. We need to show that T has a model. By (iii) $\Rightarrow$ (i) of the Main Lemma this amounts to proving that $T \cup T_{\text{Henkin}} \cup \text{Eq}$ is consistent in the sense of propositional logic. But, by the Compactness Theorem for Propositional Logic, it suffices to prove that for every finite subset $T_0 \subseteq T$, $T_0 \cup T_{\text{Henkin}} \cup \text{Eq}$ is consistent, which follows from the hypothesis and (i) $\Rightarrow$ (iii) of the Main Lemma. $\square$

Other proofs of this theorem appear in Chapters A.2 and A.3. It also follows directly from the Completeness Theorem below.

PROOF OF THE LÖWENHEIM–SKOLEM THEOREM (2.5). Let κ be some infinite cardinal and let L be a language with $\leq \kappa$ symbols. Since every formula of L is a finite sequence of symbols, there are $\leq \kappa$ formulas of L . Recall the definition of the witnessing expansion $L(C)$ of L , where $C = \bigcup_n C_n$. Clearly, by induction, each C_n has cardinality $\leq \kappa$ so C has cardinality $\leq \kappa$. Thus, any canonical structure for $L(C)$ has $\leq \kappa$ elements, so the desired result is an immediate consequence of (i) $\Rightarrow$ (ii) in the Main Lemma. $\square$

The Completeness Theorem for a Hilbert-style formal system H

There are several quite distinct approaches to the Completeness Theorem, corresponding to different ways of thinking about proofs. Within each of the approaches there are endless variations in the exact formulation, corresponding to which laws of thought are taken as basic, which as derived. We will ignore the minor variations. The different basic approaches are important, though, for different notions of proof lend themselves to different applications. The most important thing to remember, however, is that while there are many notions of *proof*, there is only one real notion of *provable* for first-order logic, as the Completeness Theorem shows.

The first type of formal system we discuss is a so called Hilbert-style formal system. It is usually the favorite of the mathematician because it is elegant and easy to remember. In 4.6 we sketch a Gentzen-type formal system. This type has proven very useful in analyzing the proof-theoretic strength of various mathematical theories. In a classroom situation, however, where students actually seem to enjoy working out formal proofs, the Fitch-type subordinate proof method or the Beth-type semantic tableaux are even better. The latter are discussed at length in SMULLYAN [1968].

In a Hilbert-style formal system, the emphasis is on logical *axioms*, keeping the rules of inference at a minimum. If we had taken $\exists x$ as a defined symbol, treating $\exists x$ as $\neg \forall x \neg \varphi$, the system would have been superficially even simpler. It seems somehow more to the point, however, to treat the laws of thought behind these quantifiers separately.

Let L be a fixed first-order language. All formulas below are first-order formulas of L , and all terms t are terms of L . Recall our convention in Section 3 about writing $\varphi(t/v)$, the result of replacing v by t in φ , only in case the variables in t do not occur bound in φ . We write $\varphi(t)$ for $\varphi(t/v)$ below.

Axiom Schemata of H

- (1) All tautologies,
- (2) All equality axioms,
- (3) All formulas of either of the forms

$$(\forall v \varphi(v)) \rightarrow \varphi(t), \quad \varphi(t) \rightarrow \exists v \varphi(v).$$

Rules of Inference of H

- (1) (*Modus Ponens*) From $(\varphi \rightarrow \psi)$ and φ infer ψ ,

(2) (*Generalization rules*) If the variable v is not free in φ , then:

from $\varphi \rightarrow \psi(v)$ infer $\varphi \rightarrow \forall y \psi(y)$,

from $\psi(v) \rightarrow \varphi$ infer $\exists y \psi(y) \rightarrow \varphi$.

These rules are usually written schematically as

$$\frac{(\varphi \rightarrow \psi) \quad \varphi}{\psi}$$

If v not free in φ , then:

$$\frac{\varphi \rightarrow \psi(v)}{\varphi \rightarrow \forall y \psi(y)}, \quad \frac{\psi(v) \rightarrow \varphi}{\exists y \psi(y) \rightarrow \varphi}.$$

A *proof of φ from a set of sentences T* (in the formal system **H**) is a finite sequence $\psi_1, \dots, \psi_n$ of formulas, with $\psi_n = \varphi$, each of which is either an axiom of **H**, a member of T , or else follows from earlier ψ_i by one of the three rules of inference. We say that φ is *provable from T* , and write $T \vdash \varphi$, if there is a proof of φ from T .

4.9. GÖDEL COMPLETENESS THEOREM FOR **H.** *Let T be a set of sentences of a language L . A sentence φ is provable from T if and only if φ is true in all set-theoretic structures which are models of T . In symbols, $T \models \varphi$ iff $T \vdash \varphi$.*

The easy half of the Completeness Theorem follows from the Soundness Lemma.

4.10. SOUNDNESS LEMMA. *Let t be a set of sentences, $\mathfrak{M}$ a model of T . If $\varphi(v_1, \dots, v_n)$ is provable from T , then $\mathfrak{M} \models \forall v_1 \cdots \forall v_n \varphi(v_1, \dots, v_n)$.*

PROOF. One proves, by induction on n , that if $\psi_1, \dots, \psi_n$ is a proof from T then $\mathfrak{M} \models \forall v_1 \cdots \forall v_k \psi_n(v_1 \cdots v_k)$. $\square$

In the proof of the Completeness Theorem we need the following lemma.

4.11. LEMMA. *Let T be a set of sentences.*

- (i) *If $T \vdash (\varphi \rightarrow \psi)$ and $T \vdash (\neg \varphi \rightarrow \psi)$, then $T \vdash \psi$.*
- (ii) *If $T \vdash (\varphi \rightarrow \theta) \rightarrow \psi$, then $T \vdash (\neg \varphi \rightarrow \psi)$ and $T \vdash (\theta \rightarrow \psi)$.*
- (iii) *If v does not appear in ψ and if $T \vdash [(\exists y \varphi(y) \rightarrow \varphi(v)) \rightarrow \psi]$, then $T \vdash \psi$.*
- (iv) *If v does not appear in ψ and if $T \vdash (\varphi(v) \rightarrow \forall y \varphi(y)) \rightarrow \psi$, then $T \vdash \psi$.*

PROOF. (i) Notice that $[(\varphi \rightarrow \psi) \rightarrow ((\neg\varphi \rightarrow \psi) \rightarrow \psi)]$ is a tautology. Thus, if we write a proof of $(\varphi \rightarrow \psi)$ and apply modus ponens we get a proof of $(\neg\varphi \rightarrow \psi) \rightarrow \psi$. Then write a proof of $(\neg\varphi \rightarrow \psi)$ and apply modus ponens to get a proof of ψ .

(ii) Note, $[((\varphi \rightarrow \theta) \rightarrow \psi) \rightarrow (\neg\varphi \rightarrow \psi)]$ and $[((\varphi \rightarrow \theta) \rightarrow \psi) \rightarrow (\theta \rightarrow \psi)]$ are tautologies.

(iii) Suppose $T \vdash [(\exists y \varphi(y) \rightarrow \varphi(v)) \rightarrow \psi]$, where v is not free in ψ . By (ii), $T \vdash (\neg \exists y \varphi(y) \rightarrow \neg \psi)$ and $T \vdash \varphi(v) \rightarrow \psi$. Apply the second generalization rule and we have $T \vdash (\exists y \varphi(y) \rightarrow \psi)$. But then by (i), $T \vdash \psi$. The proof of (iv) is similar, but uses the first generalization rule. $\square$

PROOF OF THE COMPLETENESS THEOREM. Suppose that $T \models \varphi$. By the Main Lemma (4.8) and the Compactness Theorem for propositional logic, there is a finite set $S \subseteq T \cup T_{\text{Henkin}} \cup \text{Eq}$ such that $S \cup \{\neg\varphi\}$ is inconsistent in the sense of propositional calculus. List the members of S in a list $\alpha_1, \dots, \alpha_N, \beta_1, \dots, \beta_M$ as follows. The sequence $\alpha_1, \dots, \alpha_N$ consists of those members of S which are either in $T \cup \text{Eq}$ or else are quantifier axioms (types III and IV) listed in any order. The β 's are the members of S which are Henkin axioms of types I, II, but we must list them more carefully. Recall the languages $L = L_0 \subset L_1 \subset \dots$ such that $L(C) = \bigcup_n L_n$. Define the rank of $\varphi \in L(C)$ to be the least n such that $\varphi \in L_n$. Now, choose for β_1 a Henkin axiom in S of maximum rank. Choose for β_2 a Henkin axiom in $S - \{\beta_1\}$ of maximum rank, etc. The point of arranging things in this way is that the witnessing constant about which β_i speaks, is not mentioned in $\beta_{j+1}, \dots, \beta_M$. For example, if β_1 is

$$\exists v \eta(v) \rightarrow \eta(c_{\eta(v)}),$$

then $c_{\eta(v)}$ does not appear in any of the other $\beta_2, \dots, \beta_M$, by the maximality condition on β_1 .

Recalling that $S \cup \{\neg\varphi\}$ is not consistent in the sense of propositional logic, and associating parentheses to the right, we see that

$$(\alpha_1 \rightarrow \alpha_2 \rightarrow \dots \rightarrow \alpha_N \rightarrow \beta_1 \rightarrow \dots \rightarrow \beta_M \rightarrow \varphi)$$

is a tautology. Replace each witnessing constant in this sentence by a distinct new variable. The result is still a tautology:

$$\alpha'_1 \rightarrow \alpha'_2 \rightarrow \dots \rightarrow \alpha'_N \rightarrow \beta'_1 \rightarrow \dots \rightarrow \beta'_M \rightarrow \varphi'$$

but $\varphi' = \varphi$ since φ has no witnessing constants in it. Each $\alpha'_1, \dots, \alpha'_N$ is either a logical axiom or else is a member of T , so we may apply modus ponens N times and obtain a proof of:

$$\beta'_1 \rightarrow \dots \rightarrow \beta'_M \rightarrow \varphi.$$

But now we apply parts (iii) and (iv) of Lemma 4.11 to successively remove $\beta'_1, \beta'_2, \dots, \beta'_M$ and obtain a proof of φ . $\square$

Notice that our proof used only the derived rules 4.11 (iii), (iv) so we could have used them in place of the more standard rules of **H**. This is discussed in SMULLYAN [1968].

The Completeness Theorem for a Gentzen-type formal system G^+

Hilbert-style systems are easy to define and admit a simple proof of the Completeness Theorem but they are difficult to use. Gentzen systems reverse this situation by emphasizing the importance of inference rules, reducing the role of logical axioms to an absolute minimum.

We use Γ, Δ to range over finite sets of formulas. A *sequent* is a pair $\langle \Gamma, \Delta \rangle$ which is written $\Gamma \vdash \Delta$ and read, informally, as Γ yields Δ or, rather, the *conjunction* of all the formulas in Γ yields the *disjunction* of all the formulas in Δ . We write Γ, φ for $\Gamma \cup \{\varphi\}$.

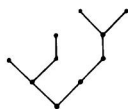
We first restrict attention to propositional logic.

Axioms: $\Gamma, \varphi \vdash \Delta, \varphi$.

Rules:

$$\begin{array}{ll}
 (\wedge \vdash) \quad \frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, (\varphi \wedge \psi) \vdash \Delta} & (\vdash \wedge) \quad \frac{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, (\varphi \wedge \psi)} \\
 (\vee \vdash) \quad \frac{\Gamma, \varphi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, (\varphi \vee \psi) \vdash \Delta} & (\vdash \vee) \quad \frac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, (\varphi \vee \psi)} \\
 (\neg \vdash) \quad \frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg \varphi \vdash \Delta} & (\vdash \neg) \quad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg \varphi} \\
 (\rightarrow \vdash) \quad \frac{\Gamma \vdash \Delta, \varphi \quad \Gamma, \psi \vdash \Delta}{\Gamma, (\varphi \rightarrow \psi) \vdash \Delta} & (\vdash \rightarrow) \quad \frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, (\varphi \rightarrow \psi)}
 \end{array}$$

A *derivation* in this system is a finite tree of formulas like, e.g.



with axioms at the upper nodes and such that each sequent on the tree follows from the ones immediately above it by one of the rules. Rather than define this precisely, we give an example, a derivation of the sequent $((\varphi \wedge \neg \psi) \vee \theta) \vdash (\varphi \vee \theta)$:

$$\begin{array}{c}
\frac{\varphi, \neg\psi \vdash \varphi, \theta}{(\varphi \wedge \neg\psi) \vdash \varphi, \theta} \quad (\text{axiom}) \\
\frac{(\varphi \wedge \neg\psi) \vdash \varphi, \theta}{(\varphi \wedge \neg\psi) \vdash (\varphi \vee \theta)} \quad (\text{by } \wedge \vdash) \quad \frac{\theta \vdash \varphi, \theta}{\theta \vdash (\varphi \vee \theta)} \quad (\text{axiom}) \\
\frac{(\varphi \wedge \neg\psi) \vdash (\varphi \vee \theta) \quad \theta \vdash (\varphi \vee \theta)}{((\varphi \wedge \neg\psi) \vee \theta) \vdash (\varphi \vee \theta)} \quad (\text{by } \vee \vdash)
\end{array}$$

4.12. THE COMPLETENESS THEOREM FOR THE PROPOSITIONAL FRAGMENT OF G. *Let Γ, Δ be finite sets of propositional formulas. The following are equivalent:*

- (i) *Every truth assignment ν making all $\varphi \in \Gamma$ true makes at least one $\psi \in \Delta$ true.*
- (ii) *There is a derivation of $\Gamma \vdash \Delta$ using the above axioms and rules.*

PROOF. The proof of (ii) $\Rightarrow$ (i) is easy by induction on the length of the derivation. For the proof of (i) $\Rightarrow$ (ii), start with a pair (Γ, Δ) satisfying (i). We attempt to build a derivation of $\Gamma \vdash \Delta$ by working backwards. At each step, we work on a formula in $\Gamma \cup \Delta$ of maximal length, breaking it apart by means of one of the rules. For example, if $(\psi \rightarrow \theta) \in \Gamma$ is the longest formula in $\Gamma \cup \Delta$ then, at the first stage, we write down

$$\frac{\Gamma_0 \vdash \Delta, \psi \quad \Gamma_0, \varphi \vdash \Delta}{\Gamma_0, (\psi \rightarrow \theta) \vdash \Delta} \quad (\rightarrow \vdash)$$

where $\Gamma_0 = \Gamma - \{(\psi \rightarrow \theta)\}$. We now work on $\Gamma_0 \vdash \Delta, \psi$ and $\Gamma_0, \varphi \vdash \Delta$ separately. Eventually we end up with sequents which cannot be broken down further. If each of the sequents on the ends is an axiom, i.e., has a prime formula common to both sides, then we have constructed a derivation of $\Gamma \vdash \Delta$. So suppose that one of these end nodes $\Gamma' \vdash \Delta'$ is not an axiom. Define ν on $\Gamma' \cup \Delta'$ by

$$\nu(p) = \begin{cases} \mathbf{t} & \text{if } p \in \Gamma', \\ \mathbf{f} & \text{if } p \in \Delta' \end{cases}$$

and define ν arbitrarily on other prime formulas. This is possible since $\Gamma' \cap \Delta' = \emptyset$. A case by case examination of the rules shows that every sequent $\Gamma'' \vdash \Delta''$ beneath $\Gamma' \vdash \Delta'$ also gets $\mathbf{t}$ assigned to everything on the left by $\bar{\nu}$ but $\mathbf{f}$ to everything on the right. In particular, this happens to $\Gamma \vdash \Delta$, a contradiction. $\square$

To pass from propositional logic to first-order logic we add equality axioms, an equality rule and four quantifier rules.

Equality axioms: $\Gamma \vdash \Delta, (t = t)$ (t any term).

Equality rule: If E is $(t_1 = t_2)$ or $(t_2 = t_1)$, then

$$\frac{\Gamma, \varphi(t_1) \vdash \Delta, \psi(t_1)}{\Gamma, E, \varphi(t_2) \vdash \Delta, \psi(t_2)},$$

$$(\forall \vdash) \frac{\Gamma, \varphi(t) \vdash \Delta}{\Gamma, \forall v \varphi(v) \vdash \Delta}, \quad (\vdash \exists) \frac{\Gamma \vdash \Delta, \varphi(t)}{\Gamma \vdash \Delta, \exists v \varphi(v)}$$

In the next two rules, *the variable v is not allowed to occur free in $\Gamma \cup \Delta$* :

$$(\vdash \forall) \frac{\Gamma \vdash \Delta, \varphi(v)}{\Gamma \vdash \Delta, \forall y \varphi(y)}, \quad (\exists \vdash) \frac{\Gamma, \varphi(v) \vdash \Delta}{\Gamma, \exists y \varphi(y) \vdash \Delta}.$$

The formal system $\mathbf{G}$ has the above axioms and rules of inference. The system $\mathbf{G}^+$ has, in addition, a rule called “cut” which is the counterpart of modus ponens:

$$\text{cut: } \frac{\Gamma, \varphi \vdash \Delta \quad \Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta}$$

Given a set T of sentences of L , we say that a formula φ is derivable from T in $\mathbf{G}^+$ if there is a derivation of $\Gamma \vdash \{\varphi\}$ for some finite $\Gamma \subseteq T$.

4.13. THE COMPLETENESS THEOREM FOR $\mathbf{G}^+$. *A sentence φ is derivable from a set T of sentences in the system $\mathbf{G}^+$ iff $T \models \varphi$.*

PROOF. The $(\Rightarrow)$ direction follows by a Soundness Lemma entirely analogous to 4.10. To prove $(\Leftarrow)$ we use the Main Lemma, the Compactness Theorem for propositional logic and 4.12. By the Main Lemma and the Compactness Theorem for Propositional Logic, there is a finite $S \subseteq T \cup T_{\text{Henkin}} \cup \text{Eq}$ such that every truth valuation ν making S true makes φ true. Using the exact notation as in the proof of 4.9, let $S = \{\alpha_1, \dots, \alpha_N, \beta_1, \dots, \beta_N\}$, and let $\alpha'_1, \dots, \alpha'_N, \beta'_1, \dots, \beta'_N$ be as before. Thus, if $\Gamma = \{\alpha'_1, \dots, \alpha'_N, \beta'_1, \dots, \beta'_N\}$, we see that $\Gamma \vdash \varphi$ is derivable in $\mathbf{G}^+$ using only the axioms and rules of propositional logic, by 4.12. Let $\Gamma_0 = \{\alpha'_1, \dots, \alpha'_k\}$, $K \leq N$, be the subset of $\{\alpha'_1, \dots, \alpha'_N\}$ of members of T . We can turn the derivation of $\Gamma \vdash \varphi$ into a derivation of $\Gamma_0 \vdash \varphi$ by means of the following claims.

- (1) If α is an equality axiom or a quantifier axiom III or IV, then $\emptyset \vdash \varphi$.
- (2) If $\Gamma \vdash \Delta$, then $\Gamma \cup \Gamma' \vdash \Delta \cup \Delta'$.

These are simple and from them we obtain $\Gamma_0 \vdash \alpha'_i$ for all $J < i \leq N$ so we can apply cut $N - J$ times and get a derivation of $\Gamma_0 \cup \{\beta'_1, \dots, \beta'_N\} \vdash \varphi$.

- (3) If $\Gamma, (\varphi \rightarrow \theta) \vdash \Delta$, then $\Gamma \vdash \Delta, \varphi$ and $\Gamma, \theta \vdash \Delta$.

This is similar to 4.11(ii). We prove the first.

$$\begin{array}{c}
 \vdots \\
 \hline
 \Gamma, \varphi \rightarrow \theta \vdash \Delta \quad (\text{hypothesis}) \qquad \Gamma, \varphi \vdash \Delta, \theta, \varphi \mid \quad (\text{axiom}) \\
 \hline
 \Gamma, \varphi \rightarrow \theta \vdash \Delta, \varphi \quad (\text{by 2}) \qquad \Gamma \vdash \Delta, (\varphi \rightarrow \theta), \varphi \quad (\vdash \rightarrow) \\
 \hline
 \Gamma \vdash \Delta, \varphi \quad (\text{cut})
 \end{array}$$

The second is similar. Combining these, the rules $(\vdash \forall)$ and $(\exists \vdash)$, and cut we obtain:

(4) If $\Gamma, \exists y \varphi(y) \rightarrow \varphi(v) \vdash \Delta$ and v is not free in $\Gamma \cup \Delta$, then $\Gamma \vdash \Delta$.

(5) If $\Gamma, \varphi(v) \rightarrow \forall v \varphi(v) \vdash \Delta$ and v not free in $\Gamma \cup \Delta$, then $\Gamma \vdash \Delta$.

Using these derived rules we remove $\beta'_1, \dots, \beta'_M$ from the hypothesis and obtain a derivation of $\Gamma_0 \vdash \varphi$. $\square$

We have used the cut rule heavily in our proof of the Completeness Theorem for $\mathbf{G}^+$, but it did not enter into the proof for the propositional part. Is it really necessary? No. One can, by working directly with the system $\mathbf{G}$, and expanding on the proof of the propositional part, prove the completeness of the system $\mathbf{G}$. See, e.g. SMULLYAN [1968]. This shows that the cut rule can be eliminated. Historically, things went the other way round, and constituted the first important chapter in proof theory after Gödel's Incompleteness Theorems.

4.14. CUT-ELIMINATION THEOREM (Gentzen). *Any sequent which has a derivation with the cut rule has one without it. I.e., $\mathbf{G}^+$ and $\mathbf{G}$ have the same derivable sequents.*

Gentzen's proof was by a complicated double induction, showing how to transform any derivation allowing the cut rule into a derivation without cut. By analyzing such inductive proofs one is able to obtain precise least upper bound to the methods of induction which are provable in first-order arithmetic. This topic is treated in detail in Chapter D.2 on cut-elimination. The system used there is simpler since only formulas in so called "negation normal form" are considered.

This concludes our discussion of the Completeness Theorem. We leave the reader with the instructive exercise of proving $\exists y [\varphi(y) \rightarrow \forall x \varphi(x)]$ in the systems $\mathbf{H}$, $\mathbf{G}$ and $\mathbf{G}^+$. The informal proof is: pick y so that $\neg \varphi(y)$, if there is such a y ; otherwise let y be arbitrary. Thus, if $\varphi(y)$, then $\forall x \varphi(x)$. The proof in $\mathbf{G}^+$ is similar.

5. Beyond first-order logic

Many logicians would contend that there is no logic beyond first-order logic, in the sense that when one is forced to make all one's mathematical (extra-logical) assumptions explicit, these axioms can always be expressed in first-order logic, and that the informal notion of *provable* used in mathematics is made precise by the formal notion *provable in first-order logic*. Following a suggestion of Martin Davis, we refer to this view as *Hilbert's Thesis*.

The first part of Hilbert's Thesis, that all of classical mathematics is ultimately expressible in first-order logic, is supported by empirical evidence. It would indeed be revolutionary were someone able to introduce a new notion which was obviously part of logic. The second part of Hilbert's Thesis would seem to follow from the first part and Gödel's Completeness Theorem. Thus Hilbert's Thesis is, to some extent, accepted by many mathematical logicians.

Even those who accept Hilbert's Thesis in theory, however, are a far cry from accepting it in practice. It would be completely impractical and, in fact, counter-productive, to always make all one's extra-logical assumptions explicit.

Let us reconsider a couple of examples from Section 2.

Example. The axiom $\forall x \exists n \geq 1 (nx = 0)$ expressing the torsion property for abelian groups is not a first-order axiom (by 2.3). If we were to apply Hilbert's Thesis in this case, we would have to axiomatize not only group theory but also the properties of natural numbers needed to carry out the arguments we were after. This would mean that the theory of torsion groups encompasses all of first-order number theory, something clearly not in the spirit of modern algebra.

Example. The notions of metric space and Hilbert space are relatively simple, modulo the ordered field $\mathbb{R}$ of real numbers. As we saw in Section 2, however, $\mathbb{R}$ is only categorical relative to set theory. It would be counter productive, though, even to pretend to formulate all ones theorems about metric spaces within some formal system of set theory, when most of what one wants to do is first-order modulo the field $\mathbb{R}$. There is no point in saddling the study of metric spaces with any more of the problems inherent in set theory, unsolvable problems the likes of which mathematics has never known before, than necessary.

The examples show that it is common mathematical practice to accept certain notions and structures as basic and work axiomatically from there on, even when we are aware that these notions cannot be completely axiomatized in the restricted language of first-order logic in and of themselves. The algebraist constantly takes the notion *finite* as basic. The student of analysis, metric spaces and Hilbert spaces begins with the structure $\mathbb{R}$ of reals. Logicians have developed strengthenings of first-order logic which allow him to be more faithful to this mathematical practice, logics which absorb certain mathematical notions, or structures, into the logic, in the same way that the algebraist attempts to absorb the notion of *finite* into his informal logic. In this section we briefly discuss some of these extensions of first-order logic.

5.1. Many-sorted first-order logic

Two-sorted first-order logic is just like ordinary first-order logic except that one has two distinct sorts of variables. For example, the natural way of writing the axioms for vector spaces is to have one sort of variable $r, s, t, \dots$ over scalars (elements of a field $\mathfrak{F}$) and a different sort $v, w, \dots$ over vectors. A vector space consists of a triple $(\mathfrak{F}, \mathfrak{V}, \cdot)$ where $\mathfrak{F}$ is a field, $\mathfrak{V} = \langle V, +, 0 \rangle$ the structure of vectors with vector addition, and the operation $\cdot$ of scalar multiplication. In general, a two-sorted structure $(\mathfrak{M}, \mathfrak{N}, \dots)$ consists of two ordinary structures plus some functions and relations on their union. Two-sorted (or many-sorted) logic is only superficially stronger, though often more natural, than ordinary logic, since we can always take a structure $(\mathfrak{M}, \mathfrak{N}, \dots)$ and turn it into an ordinary structure $\langle M \cup N, M, N, \dots, \dots, \dots \rangle$ with unary predicates M and N to sort out the different sorts of elements. This reduction allows most results of first-order logic to be transferred to many-sorted logic, and is part of the evidence for Hilbert's Thesis. Malcev and Feferman, among others, have stressed the advantages of working directly with the many-sorted case. A good introduction can be found in FEFERMAN [1974].

5.2. ω -logic

If we take a two-sorted language and consider two-sorted structures $(\mathfrak{M}, \mathfrak{N}, \dots)$ with a *fixed structure* $\mathfrak{N}$, then we obtain so called $\mathfrak{N}$ -logic. For example, $\mathbb{R}$ -logic is appropriate to the study of metric spaces and real Hilbert spaces. For $\mathbb{N}$ the structure of natural numbers, $\mathbb{N}$ -logic is usually called ω -logic. It is appropriate to the study of, say, Euclidean rings, since a Euclidean ring is a ring $\mathfrak{N}$ with a function $d : \mathfrak{N} \rightarrow \mathbb{N}$ satisfying the usual first-order axioms. As long as $\mathfrak{N}$ is infinite, $\mathfrak{N}$ -logic is stronger than

first-order logic. For example, the Compactness Theorem must fail for $\aleph$ -logic.

5.3. Weak second-order logic

Weak second-order logic is an attempt to build the notion of *finite* into logic in a natural way. Let L be a given first-order language. Let x, y, z be the variables of L . From L we form a new two-sorted language L^* which has variables a, b, c and a membership symbol $\in$. Given a structure $\mathfrak{M} = \langle M, \dots \rangle$ for L we expand it to a structure $\text{HF}(\mathfrak{M})$ for L^* , called *the structure of hereditarily finite sets on $\mathfrak{M}$* , as follows. Let

$$\text{HF}_0(M) = \emptyset$$

$$\text{HF}_{n+1}(M) = \{\text{all finite subsets of } M \cup \text{HF}_n(M)\},$$

$$\text{HF}(M) = \bigcup_n \text{HF}_n(M).$$

Then $\text{HF}(\mathfrak{M}) = (\mathfrak{M}, \text{HF}(M), \in \upharpoonright (M \cup \text{HF}(M)))$. In weak second-order logic (more accurately called weak finite-type logic) we allow ourselves to use formulas of L^* and to interpret the set variables a, b, c over $\text{HF}(M)$. Anyone familiar with the development of intuitive set theory in, say, ZF, will realize that we can define the natural numbers in $\text{HF}(\mathfrak{M})$, and the notions of finite sequence in $\text{HF}(\mathfrak{M})$. In fact, $\text{HF}(\mathfrak{M})$ is admissible (see Chapter A.7 on admissible sets, in particular, 3.1 and 2.16), so we can define functions by recursion. In particular, all of the sentences of Section 2 which we called weak second-order are easily seen to be weak second-order in this precise sense. Weak second-order logic has essentially the same strength as ω -logic, but is much more natural in the context of algebra, since one can work directly with integers, finite set, finite sequences, etc.

5.4. Infinitary logic

Weak second-order logic attempts to absorb the notion of finite into the semantics (meaning) of the logic. It has turned out to give a more elegant theory, however, to absorb it into syntax of the logic by allowing infinite formulas, like

$$\forall x [x = 0 \vee 2x = 0 \vee \dots].$$

The logic $L_{\omega_1\omega}$ allows the additional formation rule: if Φ is a countable set of formulas then $\bigwedge \Phi$ (the conjunction of Φ) and $\bigvee \Phi$ (the disjunction of Φ) are formulas. This logic is discussed in several of the chapters in this

part of the book. The notation $L_{\omega_1\omega}$ is explained by the fact that countable ($< \omega_1$) conjunctions and disjunctions are permitted but only finite ($< \omega$) strings of quantifiers. One can think of the logic $L_{\omega_1\omega}$ as expressing those notions which are first-order modulo a countable amount of information. The Lowenheim–Skolem Theorem holds for $L_{\omega_1\omega}$, but not the Compactness Theorem. To get a Completeness Theorem, for countable theories T of $L_{\omega_1\omega}$, one must add an infinitary rule of proof.

It is easy to translate weak second-order logic into $L_{\omega_1\omega}$, but not vice-versa. In particular, in weak second-order logic there are relations which are implicitly, but not explicitly definable, something that cannot happen in first-order logic or $L_{\omega_1\omega}$, by Beth's Theorem. If one looks for the *smallest* logic containing weak second-order logic in which all implicitly definable relations are explicitly definable, then one is led to the study of admissible fragments L_A of $L_{\omega_1\omega}$, as studied in Chapter A.7.

5.5. Logic with new quantifiers

It is easy to see that all finitary propositional *connectives* are definable from the ones in first order logic, in fact from $\vee$ and $\neg$. Mostowski long ago raised the possibility of adding new *quantifiers* to first-order logic. Thus, let Q be a new symbol and allow the formation rule: if $\varphi(x)$ is a formula, so is $Qx\varphi(x)$. There are many possible interpretations of Q . For example, we could define $\mathcal{M} \models Qx\varphi(x)$ iff there are *infinitely many* x such that $\mathcal{M} \models \varphi(x)$. This logic, called $L(Q_0)$, is essentially equivalent to ω -logic and weak second-order logic.

If we define $\mathcal{M} \models Qx\varphi(x)$ iff there are *uncountably many* x such that $\mathcal{M} \models \varphi(x)$ then we obtain logic with the quantifier “there exists uncountably many”. This logic, unlike all the others mentioned earlier, has a Completeness Theorem and Compactness Theorem entirely analogous to that of ordinary first-order logic, (as long as the set L of symbols is finite or countable). Few people would claim that the notion of *uncountable* is a logical, rather than mathematical, notion, but the Completeness Theorem of KEISLER [1970] for this logic does give one pause. The notions of “many” and “most” seem almost logical and various precise mathematical notions like “measure 1”, “second category”, “infinitely many”, and “uncountably many” use the intuitive notions for motivation. The Completeness Theorem of Keisler for “there exists uncountably many” shows that this notion provides a mathematically precise model for one informal concept of “many”. Written out in English, using “many” and “few” for “uncountable” and “not uncountable” respectively, Keisler's basic axioms are:

- (1) For all y there are few x such that $x = y$.

(2) If $\varphi(x) \rightarrow \psi(x)$ for all x , and if many x satisfy φ then many x satisfy ψ .

(3) If many x satisfy $(\varphi(x) \vee \psi(x))$, then either many x satisfy φ or many x satisfy ψ .

(4) If there are only a few x for which $\exists y \varphi(x, y)$, and if for each x there are only a few y such that $\varphi(x, y)$, then there are only a few y for which $\exists x \varphi(x, y)$.

Notice that “there are many x ” is not a consequence of the axioms since the axioms hold in all structures, finite, countable, or uncountable. Sometimes, late at night, one can almost imagine some other world where such axioms are considered laws of thought in the same way that we accept the laws of first-order logic. But now we are entering the realm of science fiction, or mathematical fiction, so we had better stop.

5.6. Abstract model theory

Recent years have witnessed the foundation of a new branch of model theory. Abstract model theory steps back and surveys the whole spectrum of logics and the relationships between them. A *logic* consists of a *syntax* and a *semantics* which fit together nicely, in the sense that elementary syntactic operations (like renaming symbols) are performable and have their desired meaning. Glancing at the above examples should give one a feeling for a more precise definition (see BARWISE [1974]).

Of the above examples, weak second-order logic, $L_{\omega_1\omega}$ and $L(Q_0)$ all satisfy the Löwenheim–Skolem Theorem (Theorem 2.5 with $\kappa = \aleph_0$) but not the Compactness Theorem. On the other hand, $L(Q)$, where Q means uncountable, satisfies the Compactness Theorem but not the Löwenheim–Skolem Theorem. This is explained by one of the first, and still most striking, results of abstract model theory. A proof can be found in BARWISE [1974] where other references are also given.

5.7. THEOREM (Lindström). *First-order logic is the only logic closed under $\wedge$, $\neg$, $\exists$ which satisfies the Compactness Theorem and the Löwenheim–Skolem Theorem.*

References

- BARWISE, J.
 [1974] Axioms for abstract model theory, *Ann. Math. Logic*, 7, 221–265.
- CHANG, C.C. and H.J. KEISLER
 [1973] *Model Theory* (North-Holland, Amsterdam).

ENDERTON, H.

[1972] *A Mathematical Introduction to Logic* (Academic Press, New York).

FEFERMAN, S.

[1974] Applications of many-sorted interpolation theorems, in: *Proceedings of the Tarski Symposium* (Am. Math. Soc., Providence, R.I.) pp. 205–224.

KEISLER, H.J.

[1970] Logic with the quantifier “there exist uncountably many”, *Ann. Math. Logic*, **1**, 1–93.

SHOENFIELD, J.R.

[1967] *Mathematical Logic* (Addison-Wesley, Reading, Mass.).

SMULLYAN, R.M.

[1968] *First-Order Logic* (Springer, Berlin).

Fundamentals of Model Theory

H. JEROME KEISLER

Contents

1. Introduction	48
2. Theories	49
3. Diagrams and compactness	57
4. Löwenheim–Skolem theorems	63
5. Recursively saturated models	69
6. Large and small models	73
7. Stable theories	82
8. Model-theoretic forcing	89
9. Infinite formulas and extra quantifiers	95
References	101

1. Introduction

Model theory may be described as the union of logic and universal algebra. The leading characters are the sentences φ and the structures $\mathfrak{M}$ for a language L . As we shall see in this chapter, classical examples in algebra have led to many notions in model theory. The use of sentences as mathematical objects is a powerful tool which has led to unexpected applications outside of model theory.

For example, 300 years ago Leibniz conjectured that calculus could be developed rigorously by extending the real number system $\mathbb{R}$ to a structure ${}^*\mathbb{R}$ such that ${}^*\mathbb{R}$ contains infinitesimals but every statement true of $\mathbb{R}$ is true of ${}^*\mathbb{R}$. There was no chance of solving this problem until model theory developed to the point where the statements could be defined precisely and treated as mathematical objects. Abraham Robinson solved the problem in 1960, taking the statements to be the formulas of first order logic. In the simplest formulation one starts with the structure $\mathfrak{N}$ which has the set of reals $\mathbb{R}$ for its universe, and a symbol for each real relation and function. The first step is to form a proper elementary extension ${}^*\mathfrak{N}$ of $\mathfrak{N}$, that is, a proper extension which satisfies the same first order formulas as $\mathfrak{N}$. This elementary extension is obtained easily using general results in model theory, either the compactness theorem or the Łoś ultraproduct theorem. The surprise was the next step; Robinson showed that the early intuitive arguments with infinitesimals could be rigorously carried out in ${}^*\mathbb{R}$, and new results quickly followed. Robinson's infinitesimal analysis is presented in Chapter A.6. Other applications, mostly to algebra, are presented in other chapters.

We find two historical threads in the development of model theory. In North America these are often called western and eastern model theory, because Tarski has lived on the west coast since the 1940's, and Robinson was on the east coast from 1967 to his premature death in 1975. The distinction no longer has anything to do with geography, but it is still mathematically useful.

Western model theory is in the tradition of Skolem and Tarski. It is largely motivated by problems in number theory, analysis, and set theory. It emphasizes the set of all formulas of first order logic.

Eastern model theory is in the tradition of Malcev and Robinson. It is motivated by problems in abstract algebra, where theories usually have at most two blocks of quantifiers. It emphasizes the set of quantifier-free formulas and the set of existential formulas.

Many model theorists move back and forth between western and eastern

model theory. In fact, Tarski and Robinson made major contributions to both areas (Tarski's work on real closed fields and on equational classes are eastern model theory, while Robinson's consistency theorem and his infinitesimal analysis are western model theory).

In this chapter we shall present some of the methods of both western and eastern model theory. Many notions and results have two distinct versions, a western version dealing with arbitrary formulas, and an eastern version dealing with quantifier-free formulas. We shall often use the prefix "basic" for the eastern version to distinguish it from the western version.

The deeper proofs in model theory usually depend on the construction of a model with certain properties. The constructions almost always use one or more methods from the following list.

- Elementary chains,
- diagrams and other expansions of the language,
- compactness theorem,
- downward Löwenheim–Skolem theorem,
- omitting types theorem,
- forcing,
- ultraproducts,
- homogeneous sets.

We shall explain all but the last two in this chapter. For ultraproducts and homogeneous sets, see Chapters A.3 and A.5.

This chapter will concentrate on the simplest nontrivial language, first order logic. For some applications, many-sorted logic (logic with many sorts of variables) is more natural. Our presentation can be routinely extended to many-sorted logic but the notation would be more complicated. In the last section we indicate how our methods extend to the stronger logics where model theory has been successful.

We assume that the reader knows the material in Chapter A.1, especially the important definition of satisfaction of a formula in a structure, $\mathcal{M} \models \varphi[s]$. A useful collection of survey articles on model theory is in the book MORLEY [1973]. For further study in model theory we suggest the books CHANG and KEISLER [1973], and SACKS [1972].

2. Theories

In this section we present some of the fundamental notions of model theory. In particular we shall discuss various ways of classifying theories in first order logic. We shall build upon Chapter A.1.

We consider a first order language L . By a *theory* T in L we mean a set of sentences of L . The notion $\mathcal{M} \models T$, read $\mathcal{M}$ is a *model* of T , means that $\mathcal{M}$ is a structure for L such that every $\varphi \in T$ holds in $\mathcal{M}$. Two theories T_1 and T_2 are said to be *equivalent* if they have exactly the same models. T is *consistent*, or *satisfiable*, if it has at least one model. There are two ways in which theories commonly arise.

First, consider a class K of structures for L . The *theory* of K is the set $\text{Th}(K)$ of all sentences φ of L such that φ holds in every $\mathcal{M} \in K$. For example, if K is the class of finite groups then $\text{Th}(K)$, the theory of finite groups, is the set of all sentences true in all finite groups.

K is said to be an *elementary class*, or an EC_Δ class, if K is the class of all models of some theory T (hence of $\text{Th}(K)$). The class of all groups is an elementary class. However Proposition 4.6 in this chapter shows that the class of finite groups is not an elementary class. That is, there are infinite groups $\mathcal{M}$ which satisfy every sentence true of all finite groups. To characterize the notion of a finite group one must go beyond first order logic. Other examples of non-elementary classes are in Chapter A.1.

Given a structure $\mathcal{M}$, the *theory* of $\mathcal{M}$, $\text{Th}(\{\mathcal{M}\})$ or $\text{Th}(\mathcal{M})$, is the set of all sentences true in $\mathcal{M}$.

2.1. DEFINITION. A theory T is *complete* if T is equivalent to $\text{Th}(\mathcal{M})$ for some structure $\mathcal{M}$.

Two structures $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent*, $\mathcal{M} \equiv \mathcal{N}$, if $\text{Th}(\mathcal{M}) = \text{Th}(\mathcal{N})$. Thus $\mathcal{M} \equiv \mathcal{N}$ means that $\mathcal{M}$ and $\mathcal{N}$ satisfy exactly the same sentences.

The second way in which theories commonly arise is as simple sets of sentences. A set of sentences which is equivalent to $\text{Th}(K)$ is called a *set of axioms* for K . Examples are the theories of groups, abelian groups, divisible groups, and torsion-free groups as presented in Chapter A.1. The first two examples are finitely axiomatizable, while the last two are recursively but not finitely axiomatizable. A language L is said to be *recursive* if L is finite or countable with a recursive set of symbols.

2.2. DEFINITION. A theory T is *finitely axiomatizable* if it is equivalent to a finite set of sentences. A theory T is *recursively axiomatizable* if it is equivalent to a recursive set of sentences in a recursive language.

The compactness theorem can often be used to show that a theory is not finitely axiomatizable; see Chapters A.1 and A.3. Of course, finite ax-

iomatizability implies recursive axiomatizability. It is perhaps helpful to list some additional examples.

2.3. EXAMPLE. The following theories are finitely axiomatizable:

Groups,
abelian groups,
rings,
integral domains,
fields,
fields of characteristic p ($p \neq 0$, fixed),
ordered fields,
linear order,
lattices,
Boolean algebras,
Bernays–Gödel set theory,
the inconsistent theory.

2.4. EXAMPLE. The following theories are recursively but not finitely axiomatizable:

Divisible groups,
torsion-free groups,
fields of characteristic zero,
algebraically closed fields,
real closed fields,
finite fields (Ax [1968]),
Zermelo–Fraenkel set theory,
Peano arithmetic.

It turns out that the theory of finite groups is not even recursively axiomatizable (COBHAM [1962]).

Here is a convenient characterization of recursively axiomatizable theories. A sentence φ is a *consequence* of T , $T \models \varphi$, if every model of T is a model of φ .

2.5. THEOREM. *A theory T in a recursive language is recursively axiomatizable if and only if the set of all consequences of T is recursively enumerable.*

Usually the set of consequences of a theory T is not recursive. Church's Theorem shows that if L has at least one binary relation or function symbol, the set of consequences of the empty theory (i.e., the valid

sentences) is not recursive. The rare theories which do have recursive sets of consequences are of considerable interest.

2.6. DEFINITION. A theory T in a recursive language is *decidable* if the set of all consequences of T is recursive.

Intuitively this means that there is an algorithm for deciding whether an arbitrary φ is a consequence of T . Here is a simple but useful sufficient condition for decidability which is proved in 7.2 of Chapter C.1.

2.7. THEOREM. *Every complete recursively axiomatizable theory is decidable.*

Model theory has developed some powerful techniques for showing that a theory is complete; when the theory in question is a recursive set of sentences, we can conclude that the theory is decidable. For example, in a classical paper, TARSKI and MCKINSEY [1948] showed that the theory of real closed fields is complete and hence decidable. The problem can also be viewed as follows. Given a structure $\mathfrak{M}$ (such as the field of reals), determine whether $\text{Th}(\mathfrak{M})$ is decidable, and if so, find a recursive set of axioms. For more about decidable and undecidable theories see Chapters A.4 and C.3.

We now turn to some notions which are motivated by algebraic phenomena.

2.8. DEFINITION. A *universal formula* is a formula of the form

$$\forall x_1 \cdots \forall x_n \varphi$$

where φ has no quantifiers. A *universal theory* is a theory which is equivalent to a set of universal sentences.

$\mathfrak{N}$ is a *substructure* of $\mathfrak{M}$, $\mathfrak{N} \subseteq \mathfrak{M}$, if the universe of $\mathfrak{N}$ is a subset of the universe of $\mathfrak{M}$ and the interpretation of each relation, function, or constant symbol in $\mathfrak{N}$ is the restriction of the corresponding interpretation in $\mathfrak{M}$. Equivalently, for every atomic formula φ and assignment s in $\mathfrak{N}$,

$$\mathfrak{N} \models \varphi[s] \quad \text{iff} \quad \mathfrak{M} \models \varphi[s].$$

Given a nonempty subset $X \subseteq M$, there is a least substructure $\mathfrak{N} \subseteq \mathfrak{M}$ containing X , called the *substructure generated by X* . A *finitely generated substructure* of $\mathfrak{M}$ is a substructure generated by a finite $X \subseteq M$.

2.9. PROPOSITION. *If T is a universal theory, then every substructure of a model of T is a model of T .*

In the next section we shall prove the converse of this fact, the Łoś–Tarski Theorem.

For example, the theory of groups formulated in the language $\{+, 0, -\}$ is universal, and every substructure of a group is a group. However, when group theory is formulated in the language $\{+, 0\}$, it is no longer a universal theory because an existential quantifier is needed to assert the existence of an inverse,

$$\forall x \exists y (x + y = 0 \wedge y + x = 0).$$

When formulated in the language $\{+, 0\}$, a substructure of a group is a semigroup with unit but not necessarily a group.

Some other examples of universal theories are the theories of abelian groups, rings, integral domains, lattices, linear order, Boolean algebras, and torsion-free groups.

The western analogue of a substructure is an elementary substructure (TARSKI and VAUGHT [1957]). $\mathfrak{N}$ is an *elementary substructure* of $\mathfrak{M}$, $\mathfrak{N} < \mathfrak{M}$, if $\mathfrak{N} \subseteq \mathfrak{M}$ and for every formula φ and assignment s in $\mathfrak{N}$,

$$\mathfrak{N} \models \varphi[s] \quad \text{iff} \quad \mathfrak{M} \models \varphi[s].$$

We also call $\mathfrak{M}$ an *elementary extension* of $\mathfrak{N}$ and write $\mathfrak{M} > \mathfrak{N}$. Obviously,

$$\mathfrak{N} < \mathfrak{M} \quad \text{implies} \quad \mathfrak{N} \equiv \mathfrak{M}.$$

It is often more convenient to work with embeddings instead of substructures. An *isomorphic embedding* $f: \mathfrak{N} \rightarrow \mathfrak{M}$ is a mapping of N into M such that for every atomic formula φ and assignment s in $\mathfrak{N}$,

$$\mathfrak{N} \models \varphi[s] \quad \text{iff} \quad \mathfrak{M} \models \varphi[s \circ f].$$

f must be one-to-one because $x = y$ is atomic. Similarly an *elementary embedding* $f: \mathfrak{N} \rightarrow_{\prec} \mathfrak{M}$ is a mapping such that for every formula φ and assignment s in $\mathfrak{N}$,

$$\mathfrak{N} \models \varphi[s] \quad \text{iff} \quad \mathfrak{M} \models \varphi[s].$$

An isomorphic embedding $f: \mathfrak{N} \rightarrow \mathfrak{M}$ is called an *isomorphism* if M is the range of f , in symbols $f: \mathfrak{N} \equiv \mathfrak{M}$. This is the usual notion in algebra, and

$$f: \mathfrak{N} \equiv \mathfrak{M} \Rightarrow f: \mathfrak{N} \rightarrow_{\prec} \mathfrak{M} \Rightarrow \mathfrak{N} \equiv \mathfrak{M}.$$

Although the notion of an elementary extension is very strong, there is an abundance of examples in model theory. The following criterion is useful.

2.10. THEOREM. $\mathfrak{N} < \mathfrak{M}$ if and only if $N \subseteq M$ and for every formula

$\psi(x, y_1, \dots, y_n)$ and $a \in M$, $b_1, \dots, b_n \in N$, if $\mathcal{M} \models \psi[a, b_1, \dots, b_n]$, then there exists $b \in N$ such that $\mathcal{M} \models \psi[b, b_1, \dots, b_n]$.

Notice that the condition involves only satisfaction in the larger structure $\mathcal{N}$. To prove the theorem, one shows by an easy induction on this length of φ that for every assignment s in N ,

$$\mathcal{N} \models \varphi[s] \quad \text{iff} \quad \mathcal{M} \models \varphi[s].$$

Here are some examples using Theorem 2.10.

2.11. EXAMPLE. Let F be a field and let X, Y be infinite sets of variables with $X \subseteq Y$. Then $F[X] < F[Y]$ where $F[X]$ is the ring of polynomials in X over F , and $F(X) < F(Y)$ where $F(X)$ is the pure transcendental extension of F by X . If $G(X)$ is the group freely generated by X , then $G(X) < G(Y)$.

It is an open problem of Tarski whether $G(X) < G(Y)$, or even $G(X) \equiv G(Y)$, when X is a finite set of two or more generators.

The notion of a model-complete theory provides additional examples of elementary extensions.

2.12. DEFINITION. A theory T is said to be *model-complete* if whenever $\mathcal{M}, \mathcal{N}$ are models of T and $\mathcal{M} \subseteq \mathcal{N}$, $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$. Equivalently, every isomorphic embedding between models of T is an elementary embedding.

This notion is due to ROBINSON [1956a]. It is a central idea in eastern model theory and is the topic of Chapter A.4.

2.13. EXAMPLE. The following theories are model-complete (see Chapters A.3 and A.4). Algebraically closed fields, real closed ordered fields, atomless Boolean algebras, dense linear order. Thus, for example, the ordered field of real numbers is an elementary extension of the ordered field of real algebraic numbers.

Each of the above examples has the following property which is even stronger than model-completeness. Given a formula $\varphi(x_1, \dots, x_n)$, the notation

$$T \models \varphi(x_1, \dots, x_n)$$

means that the sentence $\forall x_1 \cdots \forall x_n \varphi$ is a consequence of T .

2.14. DEFINITION. A theory T admits *elimination of quantifiers* if every formula $\varphi(x_1, \dots, x_n)$ of L is T -equivalent to a quantifier-free formula $\psi(x_1, \dots, x_n)$ of L , that is,

$$T \models \varphi(x_1, \dots, x_n) \leftrightarrow \psi(x_1, \dots, x_n).$$

It is easy to see that every T which admits elimination of quantifiers is model-complete. In fact, for T to be model-complete it is sufficient that every formula of L is T -equivalent to a universal formula of L . We shall see in the next section that this condition is also necessary. An example of a theory which is model-complete but does not admit elimination of quantifiers is the theory of real closed fields. The order relation can be defined from the field operations but a quantifier is needed.

Eastern model theory concentrates on inductive theories, defined below.

2.15. DEFINITION. A theory T said to be *inductive* if T is equivalent to a set of $\forall\exists$ sentences, that is, sentences of the form

$$\forall x_1 \cdots \forall x_n \exists y_1 \cdots \exists y_n \psi$$

where ψ is quantifier-free.

Inductive theories are also called $\forall\exists$ theories. Most theories arising in algebra are inductive. All the theories listed in Examples 2.3 and 2.4 are inductive except finite fields, Bernays–Gödel set theory, Zermelo–Fraenkel set theory, and Peano arithmetic. The next result is the reason for the use of the name “inductive”.

2.16. PROPOSITION. *If T is inductive, then the union of any increasing chain*

$$\mathfrak{M}_0 \subseteq \mathfrak{M}_1 \subseteq \mathfrak{M}_2 \subseteq \cdots$$

of models of T is a model of T .

The proof of Proposition 2.16 is easy. The converse is deeper and will be proved in the next section.

The western analogue of a chain of structures is an *elementary chain*

$$\mathfrak{M}_0 < \mathfrak{M}_1 < \mathfrak{M}_2 < \cdots$$

Elementary chains are an extremely important construction in model theory, and several applications are given later in this chapter. Their importance is based on the following fundamental result of TARSKI and VAUGHT [1957].

2.17. ELEMENTARY CHAIN THEOREM. *The union $\mathfrak{M}$ of an elementary chain*

$$\mathfrak{M}_0 < \mathfrak{M}_1 < \mathfrak{M}_2 < \cdots$$

is an elementary extension of each structure $\mathfrak{M}_n$ in the chain.

PROOF. Show by induction on the length of formulas φ that for each n and each assignment s in $\mathfrak{M}_n$,

$$\mathfrak{M}_n \models \varphi[s] \quad \text{iff} \quad \mathfrak{M} \models \varphi[s]. \quad \square$$

It follows that for any theory T , the union of an elementary chain of models of T is a model of T . Proposition 2.16 and Theorem 2.17 hold not only for countable chains of structures, but also for uncountable chains and even for arbitrary upward directed systems of structures.

There are two ways to reduce western model theory to eastern model theory by adding extra symbols. By a *conservative extension* of a theory T in L we mean a theory $T' \supseteq T$ in an expanded language $L' \supseteq L$ such that every model $\mathfrak{M}$ of T has an expansion to a model $\mathfrak{M}'$ of T' .

2.18. THEOREM. *Every theory T has a conservative extension T' which is inductive and admits elimination of quantifiers.*

PROOF. Write $\mathbf{x}$ for $x_1, \dots, x_n$. For each formula $\varphi(\mathbf{x})$ of L , add a new relation symbol $R_\varphi(\mathbf{x})$ to L' , called a *Skolem relation* for φ . T' is the union of T and

$$\{\forall \mathbf{x} (\varphi(\mathbf{x}) \leftrightarrow R_\varphi(\mathbf{x})) : \varphi \in L\}.$$

T' is obviously a conservative extension of T . By eliminating Skolem relations, every formula $\varphi'(\mathbf{x})$ of L' is T' -equivalent to a formula $\varphi(\mathbf{x})$ of L and hence to $R_\varphi(\mathbf{x})$. Therefore T' admits elimination of quantifiers. The equivalent $\forall\exists$ axioms for T' are the sentences $R_\psi, \psi \in T$, and the sentences of the form

$$\forall \mathbf{x} (R_{\neg\varphi}(\mathbf{x}) \leftrightarrow \neg R_\varphi(\mathbf{x})),$$

$$\forall \mathbf{x} (R_{\varphi \wedge \psi}(\mathbf{x}) \leftrightarrow R_\varphi(\mathbf{x}) \wedge R_\psi(\mathbf{x})),$$

$$\forall \mathbf{x} (R_{\exists y \varphi}(\mathbf{x}) \leftrightarrow \exists y R_\varphi(\mathbf{x}, y)). \quad \square$$

2.19. THEOREM. *Every theory T has a conservative extension T' which is universal and model-complete*

PROOF. For each formula of the form $\exists y \varphi(x, y)$ in L add a new function symbol $F_{\exists y \varphi}(x)$, called a *Skolem function*; call the new language L_1 . Add to T the new axioms

$$\forall x (\exists y \varphi(x, y) \leftrightarrow \varphi(x, F_{\exists y \varphi}(x))),$$

forming the theory T_1 . Iterate the process countably many times, and let $L' = \bigcup_n L_n$, $T' = \bigcup_n T_n$. Then T' is a conservative extension of T . Using the axioms one can replace existential quantifiers by Skolem functions, so that every formula φ of L' is T' -equivalent to a universal formula φ' , hence T' is model-complete. The set of universal sentences equivalent to T' contains φ' where $\varphi \in T$, and the sentences

$$\forall x \forall y (\psi(x, y) \rightarrow \psi(x, F_{\exists y \psi}(x)))$$

where ψ is quantifier-free in L' . $\square$

The theory T' in 2.18 is sometimes called the *Morley expansion* of T , while the T' in 2.19 is called the (iterated) *Skolem expansion* of T . The Morley expansion required only a single step because every sentence of L' is T' -equivalent to a sentence of L . On the other hand in the Skolem expansion we kept getting new formulas in L_{n+1} and needed to iterate the construction countably many times. Skolem expansions play a key role in Chapter A.5.

3. Diagrams and compactness

The method of diagrams was invented by Henkin and A. Robinson around 1950. They used the method to give new proofs of the Gödel completeness theorem and obtained several other applications. A diagram of a structure $\mathfrak{M}$ is analogous to the multiplication table of a group; it is a set of sentences involving new constant symbols for the elements of $\mathfrak{M}$. Diagrams are useful because they give a way of constructing models from sets of sentences. There are two kinds of diagrams, corresponding to eastern model theory and western model theory.

3.1. DEFINITION. Let $\mathfrak{M}$ be a structure for a first order logic L . The *diagram language* of $\mathfrak{M}$ is the expansion L_M of L formed by adding a new constant symbol c_m for each element $m \in M$. The *diagram expansion* of $\mathfrak{M}$ is the structure $\mathfrak{M}_M$ for L_M such that each c_m is interpreted by m . The (*basic*) *diagram* of $\mathfrak{M}$ is the set $D(\mathfrak{M})$ of all atomic and negated atomic sentences

of L_M which are true in $\mathfrak{M}_M$. The *elementary diagram* of $\mathfrak{M}$ is the complete theory $\text{Th}(\mathfrak{M}_M)$, that is, the set of all sentences of L_M true in $\mathfrak{M}_M$.

More generally, given a subset $X \subseteq M$, the expansion L_X and structure $\mathfrak{M}_X$ are defined in the natural way. If f maps X into M , then $\mathfrak{M}_{fX}$ is the structure for L_X in which each c_x is interpreted by $f(x)$.

There is a simple but useful relationship between diagrams and embeddings.

3.2. PROPOSITION. (i) *f is an isomorphic embedding of $\mathfrak{M}$ into $\mathfrak{N}$ if and only if the expansion $\mathfrak{N}_{fM}$ is a model of the diagram of $\mathfrak{M}$. Briefly,*

$$f: \mathfrak{M} \rightarrow \mathfrak{N} \quad \text{iff} \quad \mathfrak{N}_{fM} \models D(\mathfrak{M}).$$

(ii) *f is an elementary embedding of $\mathfrak{M}$ into $\mathfrak{N}$ if and only if $\mathfrak{N}_{fM}$ is a model of the elementary diagram of $\mathfrak{M}$,*

$$f: \mathfrak{M} \rightarrow_{\prec} \mathfrak{N} \quad \text{iff} \quad \mathfrak{N}_{fM} \models \text{Th}(\mathfrak{M}_M).$$

It follows that T is model-complete if and only if for every model $\mathfrak{M}$ of T , $T \cup D(\mathfrak{M})$ is complete. This is the formulation which suggested the name model-complete to Robinson.

In model theory, the most important consequence of the completeness theorem is the compactness theorem. The completeness and compactness theorems are proved in a leisurely manner in the chapter by Barwise. To illustrate the use of diagrams we shall give a second direct proof of the compactness theorem here. Still another proof, using ultraproducts, is given in Chapter A.3. Our proof is based on the lemma below.

A theory T is said to be *finitely satisfiable* if every finite subset of T has a model.

3.3. LEMMA (HENKIN [1949]). *Let M be a nonempty set, L a first order language, and T a theory in the diagram language L_M . T is the elementary diagram of some structure $\mathfrak{M}$ with universe M if and only if:*

- (i) *T is finitely satisfiable.*
- (ii) *For each sentence φ of L_M , either $\varphi \in T$ or $(\neg \varphi) \in T$.*
- (iii) *If $\exists x \varphi(x) \in T$, then $\varphi(c_m) \in T$ for some $m \in M$.*
- (iv) *If $m, n \in M$ and $m \neq n$, then $(\neg c_m = c_n) \in T$.*

PROOF. It is obvious that every elementary diagram of a model with universe M has properties (i)–(iv). If T has properties (i)–(iv), there is a

unique model $\mathfrak{M}$ whose basic diagram is included in T . Then it follows by induction on the length of φ that each sentence φ of L_M holds in $\mathfrak{M}$ if and only if it belongs to T . $\square$

3.4. COMPACTNESS THEOREM. *Let T_0 be a set of sentences of L . If T_0 is finitely satisfiable, then T_0 has a model.*

PROOF. Let L have κ sentences and let C be a set of κ new constant symbols. κ must be infinite, so the expanded language L_C also has κ sentences, say φ_α , α an ordinal $< \kappa$. We may form an increasing chain T_α , $\alpha < \kappa$, of sets of sentences of L_C such that:

- (1) Fewer than κ constant symbols from C occur in T_α .
- (2) T_α is finitely satisfiable.
- (3) If $T_\alpha \cup \{\varphi_\alpha\}$ is finitely satisfiable, then $\varphi_\alpha \in T_{\alpha+1}$.
- (4) If $\varphi_\alpha \in T_{\alpha+1}$ and φ_α is of the form $\exists x \psi(x)$, then $\psi(c) \in T_{\alpha+1}$ for some $c \in C$.

Let $T = \bigcup_{\alpha < \kappa} T_\alpha$. T_κ has properties (i)–(iii) of Lemma 3.3. The relation

$$\{(c, d): (c = d) \in T_\kappa\}$$

is an equivalence relation on the set C . Choose a set $M \subseteq C$ containing exactly one element of each equivalence class and let T be the set of all sentences of L_M belonging to T_κ . Then T has properties (i)–(iv) of the lemma, so T is the elementary diagram of some model $\mathfrak{M}$. Since $T_0 \subseteq T_\kappa$ we have $T_0 \subseteq T$, hence $\mathfrak{M}$ is a model of T_0 . $\square$

The compactness theorem is sometimes called the local theorem or the finiteness theorem. It is more often called the compactness theorem because it says that a certain topological space is compact. Topological notation is often found to be convenient in model theory, especially in the area known as stability theory (Section 7).

Given a first order language L , let S be the set of all complete theories $\text{Th}(\mathfrak{M})$ in L . We call the elements $p = \text{Th}(\mathfrak{M}) \in S$ *points* of S . The *Stone space* of L is the set S with the following topology. For each sentence φ of L , let

$$[\varphi] = \{p \in S: \varphi \in p\},$$

and let S be the topology whose basic closed sets are the sets of the form $[\varphi]$. These sets form a closed basis because

$$[\varphi \vee \psi] = [\varphi] \cup [\psi].$$

In fact, the sets $[\varphi]$ are also open (hence clopen), because

$$[\neg \varphi] = S - [\varphi].$$

The closed sets of S are exactly the intersections of basic closed sets, and hence are the sets of the form

$$S(T) = \bigcap_{\varphi \in T} [\varphi] = \{p \in S : T \subseteq p\}$$

where T is a theory in L . S is a totally disconnected Hausdorff space, because if $p \neq q$ then there is a sentence $\varphi \in p - q$, hence

$$p \in [\varphi], \quad q \notin [\varphi], \quad [\varphi] \text{ clopen.}$$

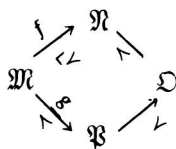
A theory T is satisfiable just in case

$$\bigcap_{\varphi \in T} [\varphi] \neq \emptyset.$$

Thus the compactness theorem states that if every finite subset of a set of basic closed sets $\{[\varphi] : \varphi \in T\}$ has a nonempty intersection, then the whole set has a nonempty intersection. In other words, the compactness theorem states that the Stone space S of L is compact.

We shall now give several applications of the compactness theorem. More applications to algebra and analysis can be found in Chapters A.1, A.3, A.4 and A.6.

3.5. THEOREM. *The amalgamation property holds for elementary embeddings. That is, if $f : \mathfrak{M} \rightarrow_{\prec} \mathfrak{N}$ and $g : \mathfrak{M} \rightarrow_{\prec} \mathfrak{P}$, then there is a structure $\mathfrak{Q}$ and a commutative diagram*



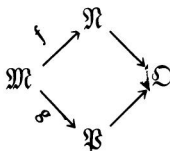
PROOF. Let $T_{\mathfrak{N}}$ and $T_{\mathfrak{P}}$ be the elementary diagrams of $\mathfrak{N}$ and $\mathfrak{P}$ with distinct constant symbols $c_n, n \in N$ and $d_p, p \in P$. Let T be the theory

$$T = T_{\mathfrak{N}} \cup T_{\mathfrak{P}} \cup \{c_{f(m)} = d_{g(m)} : m \in M\}$$

in the language $(L_{\mathfrak{N}})_{\mathfrak{P}}$. Any finite subset of T is satisfied by an expansion of $\mathfrak{M}$ to $(L_{\mathfrak{N}})_{\mathfrak{P}}$ in which the constants $c_{f(m)}, d_{g(m)}, m \in M$, are interpreted by m . Therefore by compactness, T has a model $\mathfrak{Q}'$. Let $\mathfrak{Q}$ be the reduct of $\mathfrak{Q}'$ to L , and let $h(n), k(p)$ be the interpretations of c_n, d_p in $\mathfrak{Q}'$. Then $h : \mathfrak{N} \rightarrow \mathfrak{Q}$, $k : \mathfrak{P} \rightarrow \mathfrak{Q}$, and the diagram commutes. By 3.2, h and k are elementary embeddings. $\square$

The amalgamation property for isomorphic embeddings is important in eastern model theory.

3.6. DEFINITION. A class K of structures for L has the *amalgamation property* if whenever $\mathfrak{M}, \mathfrak{N}, \mathfrak{P} \in K$ and $f: \mathfrak{M} \rightarrow \mathfrak{N}$, $g: \mathfrak{M} \rightarrow \mathfrak{P}$, there is a structure $\mathfrak{Q} \in K$ and a commutative diagram



The following result has a proof like that of Theorem 3.5.

3.7. THEOREM. *If T is a theory which admits elimination of quantifiers, then the class K of all substructures of models of T has the amalgamation property.*

We shall see later (3.11) that the class K is itself the class of models of a theory. When T and K are as in 3.7, we call T the model completion of K . Table 1 shows a short list of examples of elementary classes K with the amalgamation property. These matters are discussed further in Chapter A.4, where some exciting newer examples are discussed.

TABLE 1

K	$T =$ Model completion of K
Fields	Algebraically closed fields
Ordered fields	Real closed ordered fields
Boolean algebras	Atomless Boolean algebras
Abelian groups	Algebraically closed abelian groups
Groups	Does not exist

The next application was given by Malcev (see MALCEV [1971]) at a very early stage and was instrumental in the development of model theory. A more general treatment using ultraproducts is in Chapter A.3.

3.8. DEFINITION. A class K of structures for L is said to have *finite character* if for every $\mathfrak{M}, \mathfrak{N} \in K$ if and only if every finitely generated $\mathfrak{N} \subseteq \mathfrak{M}$ belongs to K .

3.9. THEOREM. *Suppose K is the class of all substructures of L -reducts of a theory T' in a language $L' \supseteq L$. Then K has finite character.*

PROOF. $\mathfrak{M} \in K$ if and only if $T' \cup D(\mathfrak{M})$ has a model. If every finitely generated $\mathfrak{N} \subseteq \mathfrak{M}$ belongs to K , then $T' \cup D(\mathfrak{M})$ is finitely satisfiable, and by compactness $T' \cup D(\mathfrak{M})$ has a model. $\square$

Malcev gave several applications of the above theorem to group theory. Here is a sample.

3.10. EXAMPLE. The following classes of groups have finite character by Theorem 3.9.

- (1) The class of groups with a solvable normal series of length $\leq k$ (k a fixed positive integer).
- (2) The class of groups with a normal subgroup of index $\leq k$.
- (3) The class of orderable groups, i.e. reducts of ordered groups.
- (4) The class of all groups $\mathfrak{M}$ such that for some field $\mathfrak{F}$, $\mathfrak{M}$ is representable as a group of $n \times n$ matrices over $\mathfrak{F}$.

The next theorem is the simplest example of a collection of results in model theory called preservation theorems. T is *preserved under substructures* if whenever $\mathfrak{M} \models T$, every substructure $\mathfrak{N} \subseteq \mathfrak{M}$ is a model of T .

3.11. ŁOŚ–TARSKI THEOREM. *A theory T is preserved under substructures if and only if T is a universal theory.*

PROOF. We shall prove a bit more. Let K be the class of all substructures of models of T and let $T_{\forall}$ be the set of all universal consequences of T . We prove that K is the class of all models of $T_{\forall}$. Obviously $\mathfrak{M} \in K$ implies $\mathfrak{M} \models T_{\forall}$. Let $\mathfrak{M}$ be a model of $T_{\forall}$. It follows that $D(\mathfrak{M}) \cup T$ is finitely satisfiable. By compactness $D(\mathfrak{M}) \cup T$ has a model $\mathfrak{N}$. $\mathfrak{M}$ is isomorphically embeddable in $\mathfrak{N}$ by 3.2, so $\mathfrak{M} \in K$. $\square$

By a similar argument one can prove the quantifier elimination characterization of model completeness (ROBINSON [1956a]).

3.12. THEOREM. *A theory T is model-complete if and only if every formula $\varphi(x_1, \dots, x_n)$ is T -equivalent to a universal formula $\psi(x_1, \dots, x_n)$.*

We conclude with another preservation theorem.

3.13. CHANG-ŁOŚ-SUSZKO THEOREM. *A theory T is preserved under unions of chains if and only if T is inductive, that is, equivalent to a set of $\forall\exists$ sentences.*

PROOF. For the nontrivial direction, suppose T is preserved under unions of chains. Let $T_{\forall\exists}$ be the set of $\forall\exists$ consequences of T . Consider an arbitrary model $\mathfrak{M}$ of $T_{\forall\exists}$. It follows that $D_{\forall}(\mathfrak{M}) \cup T$ is consistent, where $D_{\forall}(\mathfrak{M})$ is the set of all universal sentences of L_M true in $\mathfrak{M}_M$. By compactness, $D_{\forall}(\mathfrak{M}) \cup T$ has a model $\mathfrak{N}_M$ with $\mathfrak{M} \subseteq \mathfrak{N}$. Then every existential sentence of L_M true in $\mathfrak{N}_M$ holds in $\mathfrak{M}_M$. Hence the diagram $D(\mathfrak{N}_M)$ of $\mathfrak{N}_M$ is consistent with $\text{Th}(\mathfrak{M}_M)$. By compactness again, $\mathfrak{N}$ has an extension $\mathfrak{M}_1$ which is an elementary extension of $\mathfrak{M}$. Repeating the construction countably many times we get a chain

$$\mathfrak{M} \subseteq \mathfrak{N} \subseteq \mathfrak{M}_1 \subseteq \mathfrak{N}_1 \subseteq \cdots$$

where each $\mathfrak{N}_i$ is a model of T and the $\mathfrak{M}_i$'s form an elementary chain. The union of this chain is both a model of T and an elementary extension of $\mathfrak{M}$. Thus $\mathfrak{M}$ is a model of T , and T is equivalent to $T_{\forall\exists}$. $\square$

The method used in the above proof occurs frequently in model theory and is called the method of *alternating chains*.

3.14. COROLLARY. *Every model-complete theory is inductive, i.e. is equivalent to a set of $\forall\exists$ sentences.*

PROOF. By the elementary chain theorem and 3.13. $\square$

4. Löwenheim-Skolem Theorems

In Chapter A.1 the Löwenheim-Skolem Theorem was proved in the following form.

4.1. LÖWENHEIM-SKOLEM THEOREM. *If T has an infinite model, then T has models of every infinite cardinal κ greater than or equal to the cardinal of T .*

We shall prove two important stronger forms of this theorem due to TARSKI and VAUGHT [1957]. In this section we always let κ be an infinite cardinal greater than or equal to the number of symbols in L . By the *cardinal of $\mathfrak{M}$* we mean the cardinal $|M|$ of the universe of $\mathfrak{M}$.

4.2. DOWNWARD LÖWENHEIM-SKOLEM THEOREM. *Suppose $X \subseteq M$ and $|X| \leq \kappa \leq |M|$. Then $\mathfrak{M}$ has an elementary submodel $\mathfrak{N} < \mathfrak{M}$ of cardinal κ such that $X \subseteq N$.*

PROOF. The proof is a simple construction and does not use the compactness theorem. Form a countable increasing chain $X_0 \subseteq X_1 \subseteq X_2 \subseteq \cdots$ of subsets of M such that

(1) $X \subseteq X_0$;

(2) X_n has cardinal κ ;

(3) for each sentence $\exists x \varphi(x)$ of L_{X_n} which holds in $\mathfrak{M}_{X_n}$, there is an element of X_{n+1} which satisfies $\varphi(x)$.

Then the substructure $\mathfrak{N}$ of $\mathfrak{M}$ with universe $N = \bigcup_n X_n$ has the desired properties. $\square$

The Downward Löwenheim-Skolem Theorem has some applications which go beyond first order logic.

4.3. EXAMPLE. If a theory T in the language of ordered field theory has an Archimedean model, then it has a countable Archimedean model.

This is because every substructure of an Archimedean field is again Archimedean.

4.4. EXAMPLE. An $\in$ -model of set theory is a model of the form $\langle M, \in \rangle$. Let T be a theory in the language $L = \{\in\}$. If T has an infinite $\in$ -model, it has a countable $\in$ -model.

4.5. EXAMPLE. Let $\mathfrak{M} = \langle M, <, \dots \rangle$ be a structure such that $\langle M, < \rangle$ has order type ω_1 and the language L is countable. Then $\mathfrak{M}$ has a countable elementary submodel $\mathfrak{N}$ such that $\langle N, < \rangle$ is an initial segment of $\langle M, < \rangle$.

PROOF. Using 4.2 countably many times we obtain an elementary chain $\mathfrak{N}_0 < \mathfrak{N}_1 < \cdots$ of countable elementary submodels of $\mathfrak{M}$ such that $\mathfrak{N}_{k+1}$ contains the initial segment of M generated by $\mathfrak{N}_k$. The desired structure is the union $\mathfrak{N} = \bigcup_n \mathfrak{N}_k$ $\square$

Here is a finite analogue of the Löwenheim-Skolem Theorem.

4.6. PROPOSITION. *If a theory T has arbitrarily large finite models, then T has an infinite model.*

PROOF. The theory

$$T' = T \cup \{\forall x_1 \cdots \forall x_n \exists y (y \neq x_1 \wedge \cdots \wedge y \neq x_n): n = 1, 2, \dots\}$$

is finitely satisfiable and hence has a model. Obviously every model of T' is infinite. $\square$

We now come to another result of Tarski and Vaught, which is proved by the compactness theorem.

4.7. UPWARD LÖWENHEIM-SKOLEM THEOREM. *Let $\mathfrak{M}$ be an infinite structure for L . For every cardinal κ greater than or equal to the cardinal of $\mathfrak{M}$ and the cardinal of L , $\mathfrak{M}$ has an elementary extension of cardinal κ .*

PROOF. Let C be a set of κ new constant symbols, and form the theory T in $(L_M)_C$ given by

$$T = \text{Th}(\mathfrak{M}_M) \cup \{\neg c = d: c, d \in C, c \neq d\}.$$

T is finitely satisfiable and hence has a model $\mathfrak{N}'$. We may assume without loss of generality that for each $m \in M$, c_m is interpreted by m in $\mathfrak{N}'$. Then by 3.2, the reduct $\mathfrak{N}$ of $\mathfrak{N}'$ to L is an elementary extension of $\mathfrak{M}$. Moreover, $\mathfrak{N}$ has cardinal at least κ . By the Downward Löwenheim-Skolem Theorem there is a $\mathfrak{B}$ of cardinal κ such that $\mathfrak{M} < \mathfrak{B} < \mathfrak{N}$. $\square$

4.8. REMARK. The same method also shows that every infinite structure $\mathfrak{M}$ of cardinal κ has a proper elementary extension of cardinal κ .

The theorem is sometimes applied to an expansion of the original language L .

4.9. EXAMPLE. A *homogeneous linear ordering* is a linear ordering $\langle M, < \rangle$ such that any order-preserving function from a finite subset of M into M can be extended to an automorphism of $\langle M, < \rangle$. For every infinite κ there is a homogeneous dense linear ordering of cardinal κ .

PROOF. The ordering of the rationals, $\langle \mathbb{Q}, < \rangle$, is homogeneous. Thus for each n there is a $(2n+1)$ -placed function $f_n(x, y, z)$ such that if y and z are increasing then $f_n(\cdot, y, z)$ is an automorphism of $\langle \mathbb{Q}, < \rangle$ mapping y onto z . If $\langle M, <, \dots \rangle$ is an elementary extension of $\langle \mathbb{Q}, <, f_0, f_1, \dots \rangle$ of cardinal κ , then $\langle M, < \rangle$ is homogeneous. Of course, one can construct examples directly but they are rather complicated. $\square$

The Löwenheim–Skolem Theorem is often used in proofs that theories are complete. The simplest completeness test is the Łos–Vaught test.

4.10. DEFINITION. A theory T is said to be κ -categorical if, up to isomorphism, T has exactly one model of cardinal κ .

4.11. ŁOS–VAUGHT TEST. *If T has no finite models and T is κ -categorical for some κ , then T is complete.*

PROOF. If T has two distinct complete extensions, then T must have two nonisomorphic models of cardinal κ . $\square$

4.12. EXAMPLE. Examples of ω -categorical theories are:

- (i) Dense linear order without endpoints.
- (ii) Equivalence relations with infinitely many classes and all classes infinite.
- (iii) Atomless Boolean algebras.
- (iv) Abelian groups with all elements of order p .

4.13. EXAMPLE. Examples of ω_1 -categorical theories are:

- (i) Algebraically closed fields of given characteristic.
- (ii) Uniquely divisible torsion-free abelian groups.
- (iii) The theory of structures $\langle M, f \rangle$ where f is a permutation of M with no finite cycles.
- (iv) Abelian groups with all elements of order p .

Each of the above examples is complete (by the Łos–Vaught test) and recursively axiomatizable, and hence decidable. Theories which are κ -categorical are very rare. We shall meet them again in Sections 7 and 8. The following more general completeness test can be used more often than the Łos–Vaught test.

4.14. COMPLETENESS TEST. *A countable theory T is complete if and only if T is consistent and any two finite or countable models of T have isomorphic elementary extensions.*

PROOF. The necessity follows by compactness and the sufficiency follows from the Downward Löwenheim–Skolem Theorem. $\square$

4.15. EXAMPLE. Let T be the theory of structures $\langle M, f \rangle$ where $f : M \rightarrow M$

is a permutation of M . The complete extensions of T are exactly the theories $T(s)$ described as follows. For each countable sequence $s = \langle s_1, s_2, s_3, \dots \rangle$ of elements of $\omega \cup \{\infty\}$, let $T(s)$ be the theory of all models of T such that f has s_n cycles of length n , interpreting ∞ as infinitely many.

Case 1. $\sum s_n$ is finite. Then $T(s)$ has a unique model which is finite.

Case 2. $\sum s_n = \infty$ but only finitely many s_n are nonzero. Then $T(s)$ has no finite models and is ω -categorical, hence complete.

Case 3. Infinitely many s_n are nonzero. Let $\mathfrak{M}$ be a countable model of $T(s)$. By compactness, $\mathfrak{M}$ has a countable elementary extension $\mathfrak{N}$ with infinitely many infinite cycles. Up to isomorphism, $T(s)$ has only one such model $\mathfrak{N}$, so $T(s)$ is complete.

4.16. EXAMPLE. Let T be the theory of linear orderings in which each element has a unique successor and predecessor. The integers with order form a model of T . This theory T is complete.

We show T is complete using the method of alternating chains. Let $\mathfrak{M}$ and $\mathfrak{N}$ be two countable models of T . By compactness, there is an embedding $f: \mathfrak{M} \rightarrow \mathfrak{N}_1$ where $\mathfrak{N}_1$ is countable, $\mathfrak{N} < \mathfrak{N}_1$, and f preserves immediate successors and predecessors. Using compactness again, there is a $g: \mathfrak{N}_1 \rightarrow \mathfrak{M}_1$ where $\mathfrak{M}_1$ is countable, $\mathfrak{M} < \mathfrak{M}_1$, g preserves immediate successors and predecessors, and $f \circ g$ is the identity on M . Repeating the construction back and forth countably many times we obtain two elementary chains $\mathfrak{M} = \mathfrak{M}_0 < \mathfrak{M}_1 < \dots$ and $\mathfrak{N} = \mathfrak{N}_0 < \mathfrak{N}_1 < \dots$ such that the unions of the chains are isomorphic. Thus by 4.14, T is complete. It follows that T is the complete theory of the integers with order, and T is decidable.

Several important theories can be shown to be complete and decidable by this method. For example, the theory of the integers under addition (Pressburger), and the theory of real closed ordered fields (Tarski). The method can also be used to analyse all complete extensions of incomplete theories, for example the theory of Boolean algebras (Tarski).

There are several ways of generalizing the Löwenheim–Skolem problem by considering properties other than the cardinality of the universe of a model. The first such problem, proposed by Vaught, concerns pairs of cardinals. Suppose one of the relation symbols of L is a unary relation U . By a (κ, λ) -model we mean a model M whose universe has cardinal κ and whose interpretation of U has cardinal λ . We shall state some

Löwenheim–Skolem Theorems without proof. Some of the proofs are very deep and use infinitary combinatorics. Assume L is countable in each case.

4.17. THEOREM. *If T has a (κ, λ) -model and $\kappa \geq \kappa' \geq \lambda$, then T has a (κ', λ) -model. (This is a corollary of the Downward Löwenheim–Skolem Theorem.)*

4.18. THEOREM (CHANG and KEISLER [1973]). *If T has a (κ, λ) -model, then T has a (κ', λ') -model whenever $\kappa \geq \kappa' \geq \lambda' \geq \lambda^\omega$.*

4.19. THEOREM (VAUGHT [1965]). *If T has a (κ, λ) -model where $\lambda < \kappa$, then T has an (ω_1, ω) -model.*

4.20. THEOREM (CHANG [1965], GCH). *If T has an (ω_1, ω) -model and ω_α is a regular cardinal, then T has an $(\omega_{\alpha+2}, \omega_{\alpha+1})$ -model.*

4.21. THEOREM (JENSEN [1972], $V = L$). *If n is finite and T has an $(\omega_{\alpha+n}, \omega_\alpha)$ -model, then T has an $(\omega_{\beta+n}, \omega_\beta)$ -model.*

4.22. THEOREM (VAUGHT [1965]). *Assume $\lambda < \kappa, 2^\lambda < \kappa, 2^{2^\lambda} < \kappa, \dots$. If T has a (κ, λ) -model, then T has a (κ', λ') -model whenever $\lambda' \leq \kappa'$.*

Assuming the axiom of constructibility, $V = L$, the above results show that any “finite gap” between cardinals can be translated, any infinite gap can be replaced by an arbitrary gap, and any gap can be narrowed. Counterexamples due to FUHRKEN [1965] show that these results are best possible, that is, a finite gap cannot be made wider. Here is the counterexample for the simplest case.

4.23. EXAMPLE. Let $\mathfrak{M}$ be the ordered field of real numbers with an extra unary relation U for the set of rational numbers. $\mathfrak{M}$ is a $(2^\omega, \omega)$ -model. Since U is dense in $\mathfrak{M}$, the theory T of $\mathfrak{M}$ does not have a (κ, ω) -model for $\kappa > 2^\omega$. More generally T has no (κ, λ) -model for $\kappa > 2^\lambda$.

The situation for two-cardinal analogues of the Upward and Downward Löwenheim–Skolem Theorems is complicated and leads to independence results in set theory (see CHANG and KEISLER [1973]).

5. Recursively saturated models

The notion of a saturated model and the more recent notion of a recursively saturated model have greatly simplified and unified large parts of model theory. Intuitively, a saturated model is a model which has all possible types of elements. Saturated models were first introduced in an eastern version, which we shall call basically saturated models, by JONSSON [1960]. The western version of the notion was introduced by MORLEY and VAUGHT [1962]. The definition and main results on recursively saturated models are due to BARWISE and SCHLIPF [1976]. We shall reverse the historical order and discuss recursively saturated models in this section and saturated models in the next section.

For simplicity we assume in this section that L has only finitely many relation, function, and constant symbols. We shall require only an intuitive knowledge of recursive sets. The main facts we need are that there are only countably many recursive sets, and that any set of formulas of L which can be described by a "finite scheme" is recursive. In particular, since L has only finitely many symbols, the set of all formulas of L is recursive.

We use the notation $\Phi(x)$ to denote a set of formulas $\varphi(x)$ each with at most the single free variable x . $\Phi(x)$ is said to be *satisfiable in* $\mathfrak{M}$ if there is an element $m \in M$ which simultaneously satisfies each $\varphi(x) \in \Phi(x)$.

5.1. EXAMPLE. In ordered field theory the countable set of formulas

$$\{1 < x, 1 + 1 < x, 1 + 1 + 1 < x, \dots\}$$

is satisfiable in $\mathfrak{M}$ if and only if $\mathfrak{M}$ is nonarchimedean.

5.2. EXAMPLE. Consider the set of formulas

$$\{p(x) \neq 0: p(x) \text{ a polynomial over } \mathbf{Q}\}$$

in the theory of fields of characteristic zero. This set of formulas is satisfiable in $\mathfrak{M}$ if and only if $\mathfrak{M}$ is not an algebraic extension of the field $\mathbf{Q}$ of rational numbers.

5.3. DEFINITION. A structure $\mathfrak{M}$ is *recursively saturated* if and only if for every finite set $Y \subseteq M$, every recursive set of formulas $\Phi(x)$ in L_Y which is finitely satisfiable in $\mathfrak{M}_Y$ is satisfiable in $\mathfrak{M}_Y$.

From Example 5.1 we see that every recursively saturated ordered field is nonarchimedean. From Example 5.2, a recursively saturated field of

characteristic zero cannot be an algebraic extension of $\mathfrak{D}$. The advantage of using recursive rather than arbitrary sets of formulas is that it allows us to prove the following existence theorem.

5.4. EXISTENCE THEOREM. *Every consistent theory T in L has a finite or countable recursively saturated model.*

PROOF. Let $\mathfrak{M}_0$ be a finite or countable model of T . There are only countably many finite subsets $Y \subseteq M_0$, and for each Y there are only countably many recursive sets of formulas $\Phi(x)$ of L_Y . Thus by compactness, there is a countable elementary extension $\mathfrak{M}_1 > \mathfrak{M}_0$ such that each recursive $\Phi(x)$ finitely satisfiable in an $\mathfrak{M}_{0Y}$ is satisfiable in $\mathfrak{M}_{1Y}$. Repeat the construction countably many times. The union $\mathfrak{M} = \bigcup_{n=0}^{\infty} \mathfrak{M}_n$ is then recursively saturated, countable, and a model of T . $\square$

Recursively saturated models have several pleasant properties. The next theorem is typical.

5.5. THEOREM. *Every recursively saturated model $\mathfrak{M}$ is ω -homogeneous. That is, for any two finite tuples $a_1, \dots, a_n, b_1, \dots, b_n$ in M such that*

$$(\mathfrak{M}, a_1, \dots, a_n) \equiv (\mathfrak{M}, b_1, \dots, b_n),$$

for every $a_{n+1} \in M$ there exists $b_{n+1} \in M$ with

$$(\mathfrak{M}, a_1, \dots, a_{n+1}) \equiv (\mathfrak{M}, b_1, \dots, b_{n+1}).$$

PROOF. Let

$$Y = \{a_1, \dots, a_{n+1}, b_1, \dots, b_n\}.$$

The set of all formulas of the form

$$\varphi(a_1, \dots, a_n, a_{n+1}) \rightarrow \varphi(b_1, \dots, b_n, x)$$

is recursive and finitely satisfiable in $\mathfrak{M}_Y$, hence is satisfied by some b_{n+1} . $\square$

Countable ω -homogeneous models $\mathfrak{M}$ have the interesting property that whenever

$$(\mathfrak{M}, a_1, \dots, a_n) \equiv (\mathfrak{M}, b_1, \dots, b_n),$$

the finite mapping $a_i \rightarrow b_i$ can be extended to an automorphism of $\mathfrak{M}$.

Many of the applications of recursively saturated models use model pairs rather than single models. Given a finite language $L = \{S_1, \dots, S_n\}$, let L' and L'' be two disjoint languages with symbols of the same type as L ,

$$L' = \{S'_1, \dots, S'_n\}, \quad L'' = \{S''_1, \dots, S''_n\}.$$

Consider two structures $\mathfrak{M}, \mathfrak{N}$ for L with the same universe $M = N$. By the *model pair* $(\mathfrak{M}, \mathfrak{N})$ we mean the structure for $L' \cup L''$ whose L' -reduct is $\mathfrak{M}$ and whose L'' -reduct is $\mathfrak{N}$.

5.6. ISOMORPHISM THEOREM. *If $(\mathfrak{M}, \mathfrak{N})$ is a countable recursively saturated model pair and $\mathfrak{M} \equiv \mathfrak{N}$, then $\mathfrak{M} \cong \mathfrak{N}$.*

PROOF. Going back and forth we construct enumerations

$$M = \{a_0, a_1, \dots\}, \quad N = \{b_0, b_1, \dots\}$$

such that for each k ,

$$(\mathfrak{M}, a_1, \dots, a_k) \equiv (\mathfrak{N}, b_1, \dots, b_k).$$

When k is even we first choose a_k and then choose b_k to satisfy in $(\mathfrak{M}, \mathfrak{N})$ the recursive set of formulas

$$\varphi'(a_0, \dots, a_{k-1}, a_k) \leftrightarrow \varphi''(b_0, \dots, b_{k-1}, x),$$

where $\varphi(x_0, \dots, x_k)$ runs over formulas of L . When k is odd we choose b_k first and then a_k . $\square$

The above proof is an example of an argument which occurs frequently in model theory, called the *back and forth construction*.

One of the fundamental results in logic is the Robinson Consistency Theorem (ROBINSON [1956b]). Many proofs of this theorem have been found. Here is an especially simple proof which uses recursively saturated models.

5.7. ROBINSON CONSISTENCY THEOREM. *Let L_1 and L_2 be two expansions of the language L_0 , with $L_0 = L_1 \cap L_2$. Let T_0 be a complete theory in L_0 and let T_1, T_2 be consistent extensions of T_0 in the languages L_1 and L_2 . Then the union $T_1 \cup T_2$ is consistent.*

PROOF. Using the Löwenheim–Skolem Theorem and the existence theorem 5.4, there is a finite or countable recursively saturated model pair $(\mathfrak{M}, \mathfrak{N})$ where $\mathfrak{M}$ is a model of T_1 and $\mathfrak{N}$ a model of T_2 . $\mathfrak{M}$ and $\mathfrak{N}$ are

structures for $L_1 \cup L_2$. The reducts $\mathfrak{M}_0$ and $\mathfrak{N}_0$ of $\mathfrak{M}$ and $\mathfrak{N}$ to L_0 are models of T_0 , so $\mathfrak{M}_0 \equiv \mathfrak{N}_0$. Moreover, $(\mathfrak{M}_0, \mathfrak{N}_0)$ is still recursively saturated, so by the isomorphism theorem 5.6, $\mathfrak{M}_0 \cong \mathfrak{N}_0$. This isomorphism gives us an expansion $\mathfrak{N}_1$ of $\mathfrak{N}_0$ to L_1 which is a model of T_1 . By changing the interpretation of $L_1 - L_2$ on $\mathfrak{N}$ to fit $\mathfrak{N}_1$, we obtain a model of $T_1 \cup T_2$. $\square$

5.8. EXAMPLE. If G is a finite group, let $F(G)$ be the class of all fields $\mathfrak{M}$ such that the Galois group of $\mathfrak{M}$ over some subfield $\mathfrak{N} \subseteq \mathfrak{M}$ is G . Let T be a complete extension of field theory and let G, H be finite groups. If T has models $\mathfrak{M}_1 \in F(G)$ and $\mathfrak{M}_2 \in F(H)$, then T has a model $\mathfrak{M} \in F(G) \cap F(H)$. This is because $F(G)$ and $F(H)$ can be described by theories with extra symbols.

Many similar examples can be easily constructed.

The Robinson Consistency Theorem was also proved independently in the following equivalent form by CRAIG [1957].

5.9. CRAIG INTERPOLATION THEOREM. *Let $L = L' \cap L''$ and let φ, ψ be sentences of L and L'' . If $\varphi \rightarrow \psi$ is valid, there is a sentence θ of L such that $\varphi \rightarrow \theta$ and $\theta \rightarrow \psi$ are valid.*

PROOF. Suppose there is no such θ . Let T_0 be the set of all consequences of φ in L . Then $T_0 \cup \{\neg\psi\}$ is finitely satisfiable, and by compactness has a model $\mathfrak{M}$. Let T be the complete theory of the L -reduct of $\mathfrak{M}$. $T \cup \{\varphi\}$ and $T \cup \{\neg\psi\}$ are both consistent, so $T \cup \{\varphi, \neg\psi\}$ is consistent. But this means that $\varphi \rightarrow \psi$ is not valid. $\square$

We conclude this section with one more preservation theorem. A formula φ is *positive* if φ is built up from atomic formulas using $\wedge, \vee, \forall, \exists$. A *homomorphism* of $\mathfrak{M}$ into $\mathfrak{N}$ is a mapping f of M into N such that for each atomic formula φ and assignment s in $\mathfrak{M}$,

$$\mathfrak{M} \models \varphi[s] \text{ implies } \mathfrak{N} \models \varphi[s \circ f].$$

The substructure of $\mathfrak{N}$ whose universe is the range of f is called the *image* of the homomorphism f . We say that T is *preserved under homomorphic images* if whenever $\mathfrak{M}$ is a model of T and f is a homomorphism of $\mathfrak{M}$ into an arbitrary $\mathfrak{N}$, the image of f is a model of T .

5.10. LYNDON HOMOMORPHISM THEOREM (LYNDON [1959]). *A theory T is*

preserved under homomorphic images if and only if T is equivalent to a positive set of sentences.

PROOF. The proof that positive formulas are preserved under homomorphic images is by induction on the length of positive formulas. Assume T is preserved under homomorphic images and let T_p be the set of all positive consequences of T . Let $\mathfrak{M}$ be a model of T_p . By compactness there is a model $\mathfrak{M}'$ of T such that every positive sentence true in $\mathfrak{M}$ is true in $\mathfrak{M}'$. To avoid complications assume $\mathfrak{M}$ and $\mathfrak{M}'$ are infinite. Then there is a countable recursively saturated model pair $(\mathfrak{M}', \mathfrak{N}')$ with $\mathfrak{M} \equiv \mathfrak{M}'$, $\mathfrak{M} \equiv \mathfrak{N}'$. Using a back and forth construction we see that $\mathfrak{N}'$ is a homomorphic image of $\mathfrak{M}'$, whence $\mathfrak{N}' \models T$. Hence T_p is equivalent to T . $\square$

5.11. EXAMPLE. The theories of groups and rings are positive and are well known to be preserved under homomorphic images. The theory of integral domains is not preserved under homomorphic images (consider the integers and the integers mod n), hence its axioms cannot all be positive. The culprit is the axiom which states that there are no zero divisors,

$$\forall x \forall y (x \cdot y = 0 \rightarrow x = 0 \vee y = 0).$$

6. Large and small models

In this section we shall study two kinds of models, saturated models (which are large), and prime models (which are small). We shall first present saturated models in the original eastern version due to JONSSON [1960], and then a parallel western version due to MORLEY and VAUGHT [1962]. The theory of prime models is more successful in the western version, and in its final form is due to VAUGHT [1961]. The compactness theorem is the main tool in constructing large models. To construct small models we need a new tool, the omitting types theorem.

Jonsson's treatment applies to theories of the following kind.

6.1. DEFINITION. T is a *Jónsson theory* if:

- (i) T has an infinite model.
- (ii) T is inductive.
- (iii) T has the *joint embedding property*, that is, any two models $\mathfrak{M}, \mathfrak{N}$ of T are isomorphically embeddable in a model $\mathfrak{P}$ of T .
- (iv) $T_\forall$ has the amalgamation property.

6.2. EXAMPLE. Examples of Jónsson theories are.

Groups,
abelian groups,
Boolean algebras,
linear order,
fields of characteristic p (prime or zero),
ordered fields.

The notation $T_\forall$ denotes the set of all universal consequences of T . By a *basic formula* we shall mean a quantifier-free formula. Thus the diagram $D(\mathfrak{M})$ is equivalent to the set of all basic sentences of L_M true in $\mathfrak{M}_M$. More generally given $X \subseteq \mathfrak{M}$ we let $D(\mathfrak{M}, X)$ be the set of all basic sentences of L_X true in $\mathfrak{M}_X$. It is useful to classify elements of $\mathfrak{M}$ using the notion of a basic type.

6.3. DEFINITION. A *basic type* over T is a set of basic formulas $\Phi(x)$ with one variable which is maximal consistent with T . Given an element m of a model $\mathfrak{M}$ of T , the set of all basic formulas satisfied by m is a basic type, called the *basic type* of m .

Notice that every set of basic formulas consistent with T can be extended to a basic type over T .

6.4. EXAMPLE. Let T be the theory of fields of characteristic p (prime or zero). For each irreducible polynomial $P(x)$ over the prime field there is a basic type consisting of all consequences of $T \cup \{P(x) = 0\}$, called the type of roots of $P(x)$. T has just one more basic type, the type of the transcendental x .

The theory of ordered fields has 2^ω basic types because there are 2^ω cuts in the rationals.

6.5. DEFINITION. Let T be a Jonsson theory and κ an infinite cardinal. A model $\mathfrak{M}$ of T is *basically κ -saturated* if for each set $X \subseteq \mathfrak{M}$ of cardinal less than κ , every basic type over $T \cup D(\mathfrak{M}, X)$ is satisfied in $\mathfrak{M}_X$. (Equivalently, every set of basic formulas $\Phi(x)$ consistent with $T \cup D(\mathfrak{M}, X)$ is satisfied in $\mathfrak{M}_X$.)

$\mathfrak{M}$ is *basically saturated* if $\mathfrak{M}$ is basically κ -saturated where κ is the

cardinal of $\mathfrak{M}$ (and κ is infinite). The notion of basically κ -saturated depends on the theory T , and gets stronger as κ increases.

We state three theorems of JÓNSSON [1960]. In each case we assume T is a Jónsson theory with at most κ symbols.

6.6. EXISTENCE THEOREM. *T has a basically (κ^+) -saturated model of cardinal 2^κ .*

PROOF. The proof is like the existence theorem for recursively saturated models. We form a chain of models of length κ^+ , with models of cardinal 2^κ . At successor stages we use the amalgamation and joint embedding properties and the compactness theorem to satisfy 2^κ basic types over the previous model. $\square$

6.7 COROLLARY (GCH). *T has a basically saturated model of cardinal κ^+*

6.8. UNIQUENESS THEOREM. *Any two basically saturated models of T of the same cardinal are isomorphic.*

PROOF. By a back and forth construction. $\square$

6.9. THEOREM. *A model $\mathfrak{M}$ of T is basically κ -saturated if and only if:*

(i) *$\mathfrak{M}$ is basically κ^+ -universal. That is, any model of T of cardinal less than κ^+ is isomorphically embeddable in $\mathfrak{M}$.*

(ii) *$\mathfrak{M}$ is basically κ -homogeneous. That is, if $\mathfrak{N} \subseteq \mathfrak{M}$, $\mathfrak{N}$ is generated by a set of cardinal less than κ , and $f: \mathfrak{N} \rightarrow \mathfrak{M}$, then $\mathfrak{M}_{\mathfrak{N}}$ and $\mathfrak{M}_{f\mathfrak{N}}$ satisfy the same basic types.*

The above theorem shows the sense in which basically saturated models are large.

6.10. EXAMPLE. The basically ω_1 -saturated linear orderings are the η_1 -sets of HAUSDORFF [1914]. η_1 -sets $\langle M, < \rangle$ are dense in the strong sense that if X, Y are two subsets of cardinal less than ω_1 and $X < Y$, there exists $z \in M$ with $X < z < Y$.

It follows from ERDŐS, GILLMAN and HENRICKSON [1955] that the basically ω_1 -saturated ordered fields are exactly the real closed ordered fields whose orderings are η_1 -sets. These fields are nonarchimedean.

The basically ω_1 -saturated fields are exactly the uncountable algebraically closed fields.

If $2^\omega = \omega_1$, then there is a unique basically saturated group of cardinal ω_1 . This group turns out to be divisible and simple.

The western version of the preceding discussion is obtained by the substitutions:

Jónsson theory	→	complete theory,
diagram	→	elementary diagram,
isomorphic embedding	→	elementary embedding,
basic formula	→	formula.

In all definitions the adjective “basic” is left off. Here are the high points.

6.3'. DEFINITION. A *type* over a complete theory T is a maximal consistent set of formulas $\Phi(x)$.

6.5'. DEFINITION. A structure $\mathfrak{M}$ is κ -saturated if for each $X \subseteq M$ of cardinal less than κ , every type over $\text{Th}(\mathfrak{M}_X)$ is satisfied in $\mathfrak{M}_X$. $\mathfrak{M}$ is *saturated* if it is κ -saturated where κ is the cardinal of $\mathfrak{M}$.

6.6'. EXISTENCE THEOREM. *Every complete theory T with an infinite model has a (κ^+) -saturated model of cardinal 2^κ .*

6.8'. UNIQUENESS THEOREM. *Any two elementarily equivalent saturated structures of the same cardinal are isomorphic.*

The proofs can either be carried out directly or obtained from the previous results using the conservative expansion T' of Theorem 2.18. Recall that T' is obtained by adding a new relation symbol for each formula of L . When T is a complete theory with infinite models, T' is a Jónsson theory. Moreover, each $\mathfrak{M} \models T$ has a unique expansion $\mathfrak{M}' \models T'$, and types in $\mathfrak{M}_X$ correspond to basic types in $\mathfrak{M}'_X$.

Every ω -saturated structure for a finite language is obviously recursively saturated. Most applications of recursively saturated models are parallel to earlier applications of saturated models. Saturated models have many other applications. For example, see Chapter A.3. They are also used in the two-cardinal theorems of Chang and Jensen in Section 4, and in the Morley categoricity theorem in Section 7. One difficulty is that a countable saturated model of a theory need not exist, while a countable recursively saturated model always exists.

6.10'. EXAMPLE. The η_1 sets and η_1 real closed ordered fields are ω_1 -saturated: Every uncountable algebraically closed field is ω_1 -saturated. However, the basically saturated group of cardinal ω_1 is not saturated.

For the rest of this section we shall assume that L is a countable language, and study the countable models of complete theories in L .

We denote an n -tuple $x_1, \dots, x_n$ by $\mathbf{x}$. We shall need to consider types in n variables. By a *type in $\mathbf{x}$ over T* we mean a set of formulas $\Phi(\mathbf{x})$ maximal consistent with T . A type $\Phi(\mathbf{x})$ is *realized* in a model $\mathfrak{M}$ if it is satisfied by some $\mathbf{m}$ in $\mathfrak{M}$, and *omitted* in $\mathfrak{M}$ if it is not realized in $\mathfrak{M}$. For convenience we shall let countable mean finite or of cardinal ω , and we consider finite structures to be saturated.

We begin with a characterization of theories with countable saturated models.

6.11. THEOREM (VAUGHT [1961]). *Let T be a complete theory. Then T has a countable saturated model if and only if for each n , T has countably many types in n variables.*

PROOF. Let T have a countable saturated model $\mathfrak{M}$. Since $\mathfrak{M}$ is ω_1 -universal, every type in n variables over t is realized in $\mathfrak{M}$. Hence T has at most countably many types. The proof of the converse is like the existence proof for recursively saturated models. $\square$

6.12. COROLLARY. *If a complete theory T has only countably many nonisomorphic countable models, then T has a countable saturated model.*

6.13. EXAMPLE. The theory T of algebraically closed fields of characteristic p has countably many countable models, one of each transcendence degree n or ω . Therefore T has a countable saturated model. A model of finite transcendence degree omits any type of $n + 1$ algebraically independent elements. Thus the field of transcendence degree ω must be the saturated model.

6.14. EXAMPLE. The theory of real closed ordered fields has no countable saturated model because there are 2^ω types in one variable. Similarly, the complete theory of the standard model of arithmetic has no countable saturated model, because we get 2^ω types by considering the standard primes which divide x .

We next prove the fundamental result which allows us to construct small countable models. The most natural statement uses infinite disjunctions and conjunctions.

6.15. OMITTING TYPES THEOREM (HENKIN [1954], OREY [1956]). *Let T be a consistent theory and let $\varphi_{mn}(\mathbf{x})$, $m, n < \omega$, be formulas in $\mathbf{x}$. Assume that for each formula $\psi(\mathbf{x})$ consistent with T and each m , there exists n such that $\psi(\mathbf{x}) \wedge \varphi_{mn}(\mathbf{x})$ is consistent with T . Then T has a countable model $\mathfrak{M}$ such that*

$$\mathfrak{M} \models \bigwedge_m \forall \mathbf{x} \bigvee_n \varphi_{mn}(\mathbf{x}).$$

(The length of the sequence $\mathbf{x} = x_1 \cdots x_{f(m)}$ is independent of n .)

PROOF. We argue as in the compactness proof. Add a countable new set of constant symbols C . By listing all sentences ψ of L_C and all pairs (m, c) , we can construct a theory T' in L_C such that:

- (1) $T \subseteq T'$.
- (2) T' is complete in L_C .
- (3) If $\exists \mathbf{x} \psi(\mathbf{x}) \in T'$, then $\psi(c) \in T'$ for some $c \in C$.
- (4) For each c in C and $m < \omega$, there is an $n < \omega$ such that $\varphi_{mn}(c) \in T'$.

T' has a unique model $\mathfrak{M}'$ such that every $m \in M'$ is an interpretation of some $c \in C$. The reduct $\mathfrak{M}$ of $\mathfrak{M}'$ to L has the required property. $\square$

The original papers on the Omitting Types Theorem dealt with the special case of ω -models of arithmetic. Let L contain among its symbols the constants $\dot{0}, \dot{1}, \dot{2}, \dots$. T is said to be ω -complete if for every formula $\varphi(x)$ of L ,

$$T \models \varphi(\dot{0}), T \models \varphi(\dot{1}), \dots \text{ implies } T \models \forall x \varphi(x).$$

The infinite rule of proof which states that $\forall x \varphi(x)$ can be inferred from $\varphi(\dot{0}), \varphi(\dot{1}), \dots$ is called the ω -rule. A model $\mathfrak{M}$ of T is said to be an ω -model if every element of $\mathfrak{M}$ is equal to some constant $\dot{n}$, that is,

$$\mathfrak{M} \models \forall x \bigvee_{n < \omega} x = \dot{n}.$$

6.16. ω -COMPLETENESS THEOREM. *If T is consistent and ω -complete, then T has an ω -model.*

PROOF. If $\theta(x)$ is consistent with T , then for some $n < \omega$, $T \not\models \neg \theta(\dot{n})$. Therefore $\theta(x) \wedge x = \dot{n}$ is consistent with T , and the omitting types theorem applies. $\square$

The ω -completeness theorem also holds in the more general case of ω -logic, which has one sort of variables for natural numbers and another sort for elements (see 5.2 in Chapter A.1).

The following result was proved for models of arbitrary cardinality by MACDOWELL and SPECKER [1961]. For countable models we give a simple proof using the omitting types theorem.

6.17. THEOREM. *Let $\mathfrak{M}$ be a countable model of Peano arithmetic. Then $\mathfrak{M}$ has a proper elementary extension $\mathfrak{N}$ such that whenever $m \in M$ and $n \in N - M$ we have $m < n$.*

PROOF. Add a new constant c to L_M and let T be the theory

$$\text{Th}(\mathfrak{M}_M) \cup \{m < c : m \in M\}.$$

Using the omitting types theorem and the pigeon hole principle in Peano arithmetic, one can show that T has a model $\mathfrak{N}'$ such that

$$\mathfrak{N}' \models \bigwedge_{a \in M} \forall x \left(a \leq x \vee \bigvee_{b < a} x = b \right).$$

The reduct $\mathfrak{N}$ of $\mathfrak{N}'$ to L has the required property. $\square$

We have given two applications of the omitting types theorem to incomplete theories. We now return to our study of countable models of complete theories.

6.18. DEFINITION. A formula $\varphi(x)$ is said to be *complete* in T if the set

$$\{\psi(x) : T \models \varphi(x) \rightarrow \psi(x)\}$$

is a type over T . A type which is generated by a complete formula is called an *isolated type*.

6.19. THEOREM (VAUGHT [1961]). *Let T be a complete theory. T has a model which omits a type p if and only if p is not isolated.*

PROOF. If p is the isolated type determined by a complete formula $\varphi(x)$, then $T \models \exists x \varphi(x)$ and hence every model of T realizes p . Suppose p is not isolated. Then by the omitting types theorem, T has a model $\mathfrak{M}$ such that

$$\mathfrak{M} \models \forall x \bigvee_{\psi \in p} \neg \psi(x),$$

hence $\mathfrak{M}$ omits p . $\square$

We are ready to study small models.

6.20. DEFINITION. A *prime model* of T is a model $\mathfrak{M}$ of T which is elementarily embeddable in every model of T .

Prime models are necessarily countable, and are the opposite of ω_1 -universal models. The following results are due to VAUGHT [1961].

6.21. THEOREM. *Let T be a complete theory. $\mathfrak{M}$ is a prime model of T if and only if $\mathfrak{M}$ is countable and every type realized in $\mathfrak{M}$ is isolated.*

PROOF. Use Theorem 6.19. $\square$

6.22. UNIQUENESS THEOREM FOR PRIME MODELS. *Any two prime models of a complete theory T are isomorphic.*

The proof is again by a back and forth construction using 6.21.

6.23. EXISTENCE THEOREM FOR PRIME MODELS. *A complete theory T has a prime model if and only if every formula consistent with T belongs to an isolated type over T .*

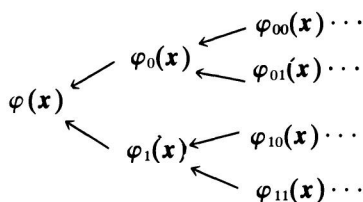
PROOF. If $\mathfrak{M}$ is a prime model of T , then any $\varphi(x)$ consistent with T is satisfied in $\mathfrak{M}$ and hence belongs to an isolated type. Assume every formula consistent with T belongs to an isolated type. Let Φ_k be the set of all complete formulas in k variables over T . By the omitting types theorem, T has a countable model $\mathfrak{M}$ such that

$$\mathfrak{M} \models \bigwedge_k \forall x \bigvee_{\varphi \in \Phi_k} \varphi(x).$$

Then by 6.21, $\mathfrak{M}$ is a prime model. $\square$

6.24. COROLLARY. *If a complete theory T has a countable saturated model, then it has a prime model.*

PROOF. Suppose T has no prime model. Let $\varphi(x)$ be consistent but not contained in an isolated type over T . Then there is a binary tree of formulas



consistent with T such that each branch of the tree can be extended to a different type. Hence T has 2^ω types in x and T has no countable saturated model. $\square$

6.25. EXAMPLE. By a process of elimination, the prime model of the theory of algebraically closed fields of characteristic p is the field of algebraic numbers. The field of real algebraic numbers is the prime model of the theory of real closed ordered fields. The standard model $\mathcal{N}$ of arithmetic is the prime model of $\text{Th}(\mathcal{N})$.

As a culmination of our study of countable saturated models we obtain a characterization of ω -categorical theories.

6.26. THEOREM (Engeler, Ryll–Nardzewski, Svenonius; VAUGHT [1961]). *Let T be a complete theory with no finite models. T is ω -categorical if and only if for each n , T has only finitely many types in n variables.*

PROOF. Assume T is ω -categorical. Let $\mathcal{M}$ be the countable model of T . By the Downward Löwenheim–Skolem Theorem, $\mathcal{M}$ is a prime model. Since every type over T is realized in $\mathcal{M}$, 6.21 shows that every type over T is isolated. If T had infinitely many types in x the set of negations of complete formulas in x would be consistent and hence contained in a type which is not isolated. Therefore T has only finitely many types in x .

Now assume that for each n , T has only finitely many types in n variables, say $p_1, \dots, p_m$. The type p_i contains the complete formula

$$\varphi = \varphi_1 \wedge \dots \wedge \varphi_m$$

where $\varphi_i \in p_i - p_j$ for $i \neq j$. Therefore each type in n variables over T is isolated. It follows from 6.21 that every countable model of T is prime, so by the uniqueness theorem for prime models, T is ω -categorical. $\square$

6.27. EXAMPLE. The theory of dense linear order is ω -categorical and

admits elimination of quantifiers. Thus for each n , the finitely many types in $x_1, \dots, x_n$ are determined by the relative order of $x_1, \dots, x_n$.

Our treatment of prime models made strong use of the fact that if a formula $\varphi(x)$ is consistent with a complete theory T , then it is satisfied in every model of T . Since Jonsson theories and basic formulas do not have this property, we do not get an analogous eastern theory for basically prime models. However, in Section 8 we shall obtain an eastern version of the omitting types theorem.

7. Stable theories

MORLEY [1965] proved the following famous theorem, answering a question of Łoś.

7.1. MORLEY CATEGORICITY THEOREM. *Let T be a theory in a countable language L . If T is categorical in some uncountable cardinal κ , then T is categorical in every uncountable cardinal λ .*

Thus for countable L there are only two kinds of κ -categoricity, ω -categoricity and ω_1 -categoricity. (The result was later extended to uncountable languages by Rowbottom, Ressayre, and ultimately SHELAH [1974].) The proof of 7.1 has been considerably simplified but is still too technical to give here. However the methods have become more important than the theorem itself. Morley gave a beautiful and fruitful classification of types over a theory. We begin with an eastern version because it has natural examples from algebra. To motivate the theory we look at extensions of fields and abelian groups.

Consider a theory T and a model $\mathfrak{M}$ of T_v . By a *basic type over $\mathfrak{M}$* we mean a basic type in one variable over the theory $T \cup D(\mathfrak{M})$. A basic type is *isolated* if it is generated by a single basic formula.

First let T be the theory of fields of given characteristic and let $\mathfrak{M}$ be a model of T . The basic types over $\mathfrak{M}$ are:

(0) For each irreducible polynomial $P(x)$ over $\mathfrak{M}$, an isolated type generated by the formula $P(x) = 0$. In an extension $\mathfrak{N} \supseteq \mathfrak{M}$, an element has one of these types if and only if it is algebraic over $\mathfrak{M}$.

(1) A single nonisolated type, realized in an extension $\mathfrak{N} \supseteq \mathfrak{M}$, by the transcendental elements over $\mathfrak{M}$.

The types (0) are said to be algebraic, or of Morley rank zero, over $\mathfrak{M}$.

The type (1) is said to be of Morley rank one over $\mathfrak{M}$. If $\mathfrak{M} \subseteq \mathfrak{N}$, each basic type over $\mathfrak{M}$ can be extended to several different basic types over $\mathfrak{N}$. However, for field theory it happens that if a basic type p over $\mathfrak{M}$ is isolated, then every extension $q \supseteq p$ over $\mathfrak{N}$ is isolated.

Now let T be the theory of abelian groups and let $\mathfrak{M} \models T$. Obviously, for each $m \in M$ the formula $x = m$ generates an isolated type, which has Morley rank zero. Another type p is generated by the set of formulas

$$\{x \neq m : m \in M\} \cup \{2x = 0\}.$$

p is the type of $x \notin M$ of order 2, and is isolated if and only if $\mathfrak{M}$ has only finitely many elements of order 2. However, over an extension $\mathfrak{N} \supseteq \mathfrak{M}$, p will always split into a set of isolated types over $\mathfrak{N}$ and at most one nonisolated type. p is an example of a type of Morley rank 1. The type of x of order 4 such that $2x \notin M$ has Morley rank 2, and so on. The type of x such that $nx \notin M$ for all n has Morley rank ω .

We are ready for the general definition. It is easier to define the Morley rank of a basic formula.

Until further notice we assume that T is a Jonsson theory in a countable language. Recall from Section 3 that $\mathfrak{M} \models T_v$ iff $\mathfrak{M}$ is a substructure of some $\mathfrak{N} \models T$.

7.2. DEFINITION. Let $\mathfrak{M}$ be a model of T_v . The (*basic*) *Morley rank* $m(\varphi)$ of a basic formula $\varphi(x)$ of L_M is defined inductively by:

- (i) $m(\varphi) = -1$ if $\varphi(x)$ is inconsistent with $T \cup D(\mathfrak{M})$.
- (ii) $m(\varphi) = 0$ if for each $\mathfrak{M} \subseteq \mathfrak{N} \models T_v$, $\varphi(x)$ belongs to finitely many basic types over $\mathfrak{N}$.
- (iii) Let α be an ordinal. $m(\varphi) = \alpha$ if for each $\mathfrak{M} \subseteq \mathfrak{N} \models T_v$, the set $\{\varphi(x)\} \cup \{\neg\psi(x) : \psi \text{ has rank } < \alpha \text{ over } \mathfrak{N}\}$ can be extended to finitely many basic types over $\mathfrak{N}$.
- (iv) $m(\varphi) = \infty$ if $m(\varphi) \neq -1$ and $m(\varphi) \neq \alpha$ for all ordinals α .

Here “finitely many” means at least one but fewer than ω .

Notice that if $T \models \varphi(x) \rightarrow \psi(x)$ then $m(\varphi) \leq m(\psi)$.

7.3. DEFINITION. The Morley rank of a basic type p over $\mathfrak{M}$ is the least α such that p contains a formula of Morley rank α .

We begin with a lemma showing that Morley ranks are well behaved.

7.4. LEMMA. Let $\mathfrak{M} \subseteq \mathfrak{N} \models T_v$, and let $\varphi(x)$ be a basic formula of L_M .

- (i) The Morley ranks of $\varphi(x)$ over $\mathfrak{M}$ and over $\mathfrak{N}$ are equal.

(ii) Let $m(\varphi) = \alpha < \infty$. Then φ belongs to finitely many basic types of rank α and no basic types of rank $> \alpha$ over $\mathfrak{M}$.

(iii) If p has rank $\alpha < \infty$ over $\mathfrak{M}$, then p can be extended to finitely many basic types of rank α and no basic types of rank $> \alpha$ over $\mathfrak{M}$.

PROOF (i) is by induction on rank using the amalgamation property of T_v . The implications (i) $\rightarrow$ (ii) and (ii) $\rightarrow$ (iii) follow easily from the definitions. $\square$

7.5. DEFINITION. The (*basic*) *Morley rank* of T is the Morley rank of the true formula $x = x$ over any model $\mathfrak{M} \models T_v$. Equivalently, the Morley rank of T is the maximum rank of a basic type over a model $\mathfrak{M} \models T_v$.

MORLEY [1965] calls theories of rank $< \infty$ *totally transcendental*.

7.6. EXAMPLE. The theory of fields of given characteristic has Morley rank one. The theory of equivalence relations $\langle M, E \rangle$ has Morley rank two. (For each $m \in M$, the type of $x \notin M$ with $E(x, m)$ has rank one, while the set of formulas $\{\neg E(x, m) : m \in M\}$ generates a type of rank two.) The theories of abelian groups and differential fields of characteristic zero have Morley rank ω . The theory of linear order has Morley rank ∞ . A linear ordering $\mathfrak{M}$ has the following types: for each $m \in M$, a type of rank zero generated by $x = m$; for each Dedekind cut of type of rank ∞ .

Perhaps the best way to understand the definition of the Morley rank is in topological terms. It is closely related to the Cantor–Bendixson derivative. In Section 3 we explained the compactness theorem with a topological space whose points are complete theories. Now we form a topological space whose points are types.

Given a Jónsson theory T and a model $\mathfrak{M}$ of T_v , let $S(\mathfrak{M})$ be the set of basic types in one variable over $\mathfrak{M}$. For each basic formula $\varphi(x)$ of L_M , let

$$[\varphi] = \{p \in S(\mathfrak{M}) : \varphi \in p\}.$$

We make $S(\mathfrak{M})$ into a topological space, the *basic Stone space over $\mathfrak{M}$* , by taking as a closed basis the sets of the form $[\varphi]$. It follows from the compactness theorem that $S(\mathfrak{M})$ is a compact totally disconnected Hausdorff space. A point $p \in S(\mathfrak{M})$ is isolated in the sense of being generated by a single basic formula if and only if it is isolated in the topological sense. Thus if $[\varphi]$ is finite, then every $p \in [\varphi]$ is isolated. The *Cantor–Bendixson derivative* of $S(\mathfrak{M})$ is the space

$$S(\mathfrak{M})' = \{p \in S(\mathfrak{M}) : p \text{ is not isolated}\}.$$

Iterating the process through the ordinals, we define

$$S(\mathfrak{M})^0 = S(\mathfrak{M}),$$

$$S(\mathfrak{M})^{\alpha+1} = (S(\mathfrak{M})^\alpha)'$$

$$S(\mathfrak{M})^\alpha = \bigcap_{\beta < \alpha} S(\mathfrak{M})^\beta \quad \text{for limit } \alpha,$$

$$S(\mathfrak{M})^\infty = \bigcap_\alpha S(\mathfrak{M})^\alpha.$$

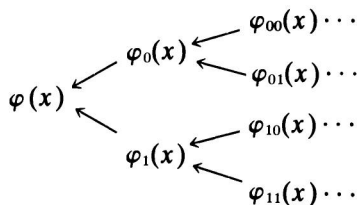
For each α , $S(\mathfrak{M})^\alpha$ is a closed set. The intersection $S(\mathfrak{M})^\infty$ is called the *perfect kernel* of $S(\mathfrak{M})$. Finally, for each $p \in S(\mathfrak{M})$, the *Cantor–Bendixson rank* of p is the greatest α such that $p \in S(\mathfrak{M})^\alpha$.

The Morley rank differs from the Cantor–Bendixson rank because the Morley rank involves arbitrary extensions $\mathfrak{N} \supseteq \mathfrak{M}$ instead of $\mathfrak{M}$ itself. One way to define the Morley rank topologically is to use the category of basic Stone spaces of models (see SACKS [1972]). A simpler way is to take $\mathfrak{M}$ to be basically ω_1 -saturated.

7.7. THEOREM. *Let $\mathfrak{M}$ be a basically ω_1 -saturated model of T . Then for every basic type $p \in S(\mathfrak{M})$, the Morley rank of p is equal to the Cantor–Bendixson rank of p .*

PROOF. To get an idea of what is going on we give the proof for rank zero. If p has Morley rank zero, then it is isolated over every $\mathfrak{N} \supseteq \mathfrak{M}$, hence isolated over $\mathfrak{M}$ and of Cantor–Bendixson rank zero. Suppose p has Morley rank greater than zero, and let $p \in [\varphi]$. Then $\varphi(x)$ has Morley rank greater than zero, so there is an $\mathfrak{N}$ such that $\varphi(x)$ belongs to infinitely many basic types over $\mathfrak{N}$, say $q_0, q_1, q_2, \dots$. These types can be distinguished by countably many formulas, so we may take $\mathfrak{N}$ to be countable. Since $\mathfrak{M}$ is basically ω_1 -saturated we may take $\mathfrak{N} \subseteq \mathfrak{M}$. Therefore $[\varphi]$ is infinite, p is not isolated, and p has Cantor–Bendixson rank > 0 . $\square$

7.8. LEMMA. *Let $\mathfrak{M}$ be a basically ω_1 -saturated model of T . A basic formula $\varphi(x)$ over $\mathfrak{M}$ has Morley rank ∞ if and only if there is a binary tree of basic formulas*



such that each branch is consistent with $T \cup D(\mathcal{M})$ but no basic type belongs to more than one branch.

PROOF. The proof is purely topological, and the lemma is a classical result on perfect kernels. For some α , $S(\mathcal{M})^\infty = S(\mathcal{M})^\alpha = S(\mathcal{M})^{\alpha+1}$, so $S(\mathcal{M})^\infty$ has no isolated points. Therefore if $m(\varphi) = \infty$, $[\varphi] \cap S(\mathcal{M})^\infty$ is infinite and may be split repeatedly to obtain a binary tree with root $\varphi(x)$.

For the converse suppose $m(\varphi) = \alpha < \infty$ and there is a binary tree with root $\varphi(x)$. We may assume α is the least such ordinal. Since $[\varphi]$ contains only finitely many points of rank α , there must be a formula $\varphi_s(x)$ in the tree of rank less than α . But $\varphi_s(x)$ is also the root of a binary tree, so we have a contradiction. $\square$

The next result of MORLEY [1965] characterizes totally transcendental theories in terms of the size of the Stone spaces.

7.9. DEFINITION. A theory T is *basically κ -stable* if for every model $\mathcal{M}$ of $T_\forall$ of cardinal κ , the basic Stone space $S(\mathcal{M})$ has cardinal κ .

7.10. THEOREM. T has Morley rank $< \infty$ if and only if T is basically ω -stable.

PROOF. If T has Morley rank ∞ , then by 7.8 there is a binary tree of basic formulas over a model $\mathcal{M}$ of T . Take a countable submodel $\mathfrak{N} \subseteq \mathcal{M}$ containing all the constants which occur in the tree. Since the tree has 2^ω branches, there are 2^ω basic types over $\mathfrak{N}$, and T is not ω -stable.

Now suppose T is not ω -stable. Then $S(\mathcal{M})$ is uncountable for some countable $\mathcal{M} \models T_\forall$. Each $\varphi(x)$ such that $[\varphi]$ is uncountable can be split into two disjoint basic sets $[\varphi_1]$ and $[\varphi_2]$ which are still uncountable, because there are only countably many formulas over $\mathcal{M}$. Hence there is a binary tree of basic formulas over $\mathcal{M}$. $\square$

7.11. COROLLARY. If T is basically ω -stable, then the Morley rank of T is countable ordinal.

PROOF. By induction on the number of generators, there are only countably many nonisomorphic finitely generated models $\mathfrak{N} \models T_\forall$. Therefore there are only countably many different Morley ranks of basic formulas over models of $T_\forall$. We can see from the definition that if there are no formulas of rank α , then there are none of rank $> \alpha$. Hence every formula has countable rank. $\square$

Notice that if T is basically κ -stable where κ is regular (perhaps ω), we can construct a basically saturated model of T of cardinal κ , even without the GCH. The work of Shelah has shown that κ -stability is of fundamental importance. He used the following classification of theories.

7.12. DEFINITION. The *basic stability spectrum* of T is the class of all infinite cardinals κ such that T is basically κ -stable.

7.13. THEOREM (SHELAH [1971]). *Every theory T has one of the following four basic stability spectra s_T .*

- (i) $s_T = \{\kappa: \omega \leq \kappa\}$ (T is basically ω -stable).
- (ii) $s_T = \{\kappa: 2^\omega \leq \kappa\}$ (T is basically superstable).
- (iii) $s_T = \{\kappa: \kappa = \kappa^\omega\}$ (T is basically stable).
- (iv) s_T is empty (T is basically unstable).

The first step of the proof, due to MORLEY [1965], proceeds as follows. Assume T is not basically κ -stable. As in the proof of Theorem 7.10, there is a binary tree of basic formulas over some model of T , hence T is not basically ω -stable. Thus ω -stability implies κ -stability for all κ . The remaining steps are much harder.

7.14. EXAMPLE. The theory of countably many unary relations is basically superstable but not ω -stable. The theory of R -modules where $R = Z \oplus Z \oplus Z \oplus \cdots$ is basically stable but not superstable. So is the theory of differential fields of prime characteristic p with a symbol for the p^{th} root (SHELAH [1971]).

A finer classification of theories is obtained using the stability function of T .

7.15. DEFINITION. The *basic stability function* of T is the function f_T on infinite cardinals κ defined by

$$f_T(\kappa) = \sup\{|S(\mathcal{M})|: \mathcal{M} \text{ is a model of } T \text{ of cardinal } \kappa\}.$$

The basic stability function of linear order is denoted by $\text{ded}(\kappa)$. Thus

$$\text{ded}(\kappa) = \sup\{\lambda: \text{There is a linear order} \\ \text{of cardinal } \kappa \text{ with } \lambda \text{ Dedekind cuts}\}.$$

7.16. THEOREM (KEISLER [1976]). *Every theory T has one of the following six basic stability functions f_T :*

- (i) $f_T(\kappa) = \kappa$ (T is basically ω -stable).
- (ii) $f_T(\kappa) = \kappa + 2^\omega$ (T is basically superstable).
- (iii) $f_T(\kappa) = \kappa^\omega$ (T is basically stable).
- (iv) $f_T(\kappa) = \text{ded}(\kappa)$ (T is basically ordered).
- (v) $f_T(\kappa) = (\text{ded } \kappa)^\omega$ (T is basically multiply ordered).
- (vi) $f_T(\kappa) = 2^\kappa$ (T is basically independent).

Each kind of theory has a syntactical characterization which suggests the name given to it. The theories (iv), (v), and (vi) are basically unstable.

7.17. EXAMPLE. The theories of linear order and ordered fields are basically ordered. The theory of countably many linear order relations is basically multiply ordered. The theories of groups, Boolean algebras, and rings are independent. For more examples see KEISLER [1976].

The classification theorems 7.13 and 7.16 hold not only for Jónsson theories but for arbitrary theories T with a slight change in the definition of the stability function.

Everything we have done in this section also holds in a western version. We assume that T is a complete theory in a countable language and everywhere remove the word “basically”.

A very rough plan of the proof of the Morley categoricity theorem is as follows. Assuming T is κ -categorical for $\kappa > \omega$, first show that T is ω -stable. Then show that the model of cardinal κ is saturated. Next, prove that if T has an uncountable model which is not saturated, then T has a model of cardinal κ which is not saturated. Hence all uncountable models of T are saturated.

Here is a characterization of ω_1 categorical theories in terms of stability. The necessity is due to MORLEY [1965] and the sufficiency to BALDWIN and LACHLAN [1971].

7.18. THEOREM. *For a complete theory T to be ω_1 -categorical it is necessary and sufficient that:*

- (i) T is ω -stable;
- (ii) for every $\mathfrak{M} \models T$ of cardinal ω_1 , every definable set in $\mathfrak{M}$ is either finite or uncountable.

The *cardinality spectrum* of a complete theory T is the function

$g_T(\kappa)$ = number of nonisomorphic models of T of cardinality κ . A very difficult problem is to determine which functions are cardinality spectra. The Morley categoricity theorem shows that for uncountable κ , $g_T(\kappa)$ is either always or never equal to one. Much more progress has been made using stability, particularly by Shelah. We state two typical results.

7.19. THEOREM (LACHLAN [1973]). *If T is superstable but not ω -categorical, then T has exactly ω nonisomorphic countable models.*

Here is a result at the opposite extreme from categoricity.

7.20. THEOREM (SHELAH [1971]). *If T is not superstable, then T has 2^κ nonisomorphic models in every uncountable cardinal κ .*

7.21. EXAMPLE. If $\mathfrak{M}$ is an infinite linear order, or an infinite Boolean algebra, then $\text{Th}(\mathfrak{M})$ is unstable and therefore has 2^κ nonisomorphic models of each uncountable cardinal κ . The result fails for $\kappa = \omega$; for example, the theories of dense linear order and atomless Boolean algebras are unstable but ω -categorical.

Some other important applications of stability are discussed in Chapters A.4 and A.5.

8. Model-theoretic forcing

We shall describe A. Robinson's finite forcing (ROBINSON [1970]). It is analogous to Cohen forcing but is a simpler construction which gives models of an arbitrary inductive theory. Forcing is closely related to the omitting types theorem in Section 6, and in fact yields an eastern version of the omitting types theorem (Theorem 8.15). For a more general theory of forcing which includes Cohen and Robinson forcing as well as the omitting types theorem, see KEISLER [1973].

The material in this section belongs to eastern model theory.

Assume throughout this section that L is a countable language and C is a countably infinite set of new constant symbols. T will always denote a consistent theory in L .

8.1. DEFINITION. By a *condition for T* we mean a finite set of atomic and

negated atomic sentences of L_C which is consistent with T . $p, q, \dots$ denote conditions for T . Notice that the empty set $\emptyset$ is a condition for T .

8.2. DEFINITION. The relation p forces φ , denoted by $p \Vdash \varphi$ or if necessary $p \Vdash_T \varphi$, is between conditions p and arbitrary sentences φ of L_C . It is defined inductively on the length of φ by:

If φ is atomic, $p \Vdash \varphi$ iff $\varphi \in p$.

$p \Vdash \neg \varphi$ iff there is no condition $q \supseteq p$ with $q \Vdash \varphi$.

$p \Vdash \exists x \varphi(x)$ iff $p \Vdash \varphi(c)$ for some $c \in C$.

$p \Vdash \varphi \vee \psi$ iff $p \Vdash \varphi$ or $p \Vdash \psi$.

In the above definition we take $\neg, \vee, \exists$ to be the fundamental symbols and regard $\wedge, \rightarrow, \leftrightarrow, \forall$ as abbreviations. The definition of forcing is just like the definition of satisfaction except for the $\neg$ clause. Intuitively, we can think of a condition p as a finite amount of information about a structure $\mathfrak{M}$. We say that p weakly forces φ , $p \Vdash^w \varphi$, if $p \Vdash \neg \neg \varphi$.

8.3. LEMMA. (i) If $p \Vdash \varphi$ and $p \subseteq q$, then $q \Vdash \varphi$.

(ii) If $\varphi \in p$, then $p \Vdash \varphi$.

(iii) $p \Vdash^w \varphi$ if and only if for all $q \supseteq p$ there exists $r \supseteq q$ with $r \Vdash \varphi$.

(iv) $p \Vdash \varphi$ implies $p \Vdash^w \varphi$.

PROOF. (i) is by induction on the length of φ , while (ii)–(iv) are immediate. $\square$

To construct models by forcing we introduce the notion of a generic set.

8.4. DEFINITION. A generic set for T is a set G of basic sentences where:

(i) Each finite $p \subseteq G$ is a condition for T .

(ii) For each sentence φ of L_C there is a condition $p \subseteq G$ such that either $p \Vdash \varphi$ or $p \Vdash \neg \varphi$.

$G \Vdash \varphi$ means that $p \Vdash \varphi$ for some $p \subseteq G$. It follows that for each φ , exactly one of $G \Vdash \varphi$, $G \Vdash \neg \varphi$ holds.

8.5. LEMMA. For each condition p there is a generic set $G \supseteq p$.

PROOF. Let $\varphi_0, \varphi_1, \dots$ be a list of all sentences of L_C . Using the negation

clause we can choose a chain of conditions $p_0 \subseteq p_1 \subseteq \dots$ such that for each n , $p_n \Vdash \varphi_n$ or $p_n \Vdash \neg \varphi_n$. Then $G = \bigcup_n p_n$ is generic. $\square$

The preceding lemma is our reason for assuming that L and C are countable. We now come to the main result of the construction

8.6. GENERIC MODEL THEOREM. *Let G be a generic set for T . There is a unique (up to isomorphism) structure $\mathfrak{M}(G)$ for L_C such that:*

- (i) *each $m \in M(G)$ is the interpretation of some $c \in C$,*
- (ii) *for each sentence φ of L_C ,*

$$\mathfrak{M}(G) \models \varphi \quad \text{iff} \quad G \Vdash \varphi.$$

That is,

$$\text{Th}(\mathfrak{M}(G)) = \{\varphi : G \Vdash \varphi\}.$$

PROOF. The relation

$$c \sim d \quad \text{iff} \quad G \Vdash c = d$$

is an equivalence relation on C . For the universe of $\mathfrak{M}(G)$ we take a set $M(G) \subseteq C$ containing exactly one element of each equivalence class. When $c \sim m \in M$ interpret c by m , and let $\mathfrak{M}(G)$ be the unique model of G with universe $M(G)$. Then (ii) holds for each atomic φ . It follows by induction on the length of φ that (ii) holds for all φ . The fact that G is generic is used in the negation step of the induction,

$$\mathfrak{M}(G) \models \neg \varphi \quad \text{iff} \quad \mathfrak{M}(G) \not\models \varphi \quad \text{iff} \quad G \nVdash \varphi \quad \text{iff} \quad G \Vdash \neg \varphi. \quad \square$$

The next corollary is useful in showing that sentences are forced.

8.7. COROLLARY. *The following are equivalent:*

- (i) $p \Vdash^w \varphi$.
- (ii) *For every generic set G for T with $p \subseteq G$, $\mathfrak{M}(G) \models \varphi$.*

We turn our attention to T -generic models.

8.8. DEFINITION. A structure $\mathfrak{M}$ for L is said to be a *T -generic model* if $\mathfrak{M}$ is isomorphic to the L -reduct of $\mathfrak{M}(G)$ for some generic set G for T .

8.9. THEOREM. *If T is an inductive theory, then every T -generic model is a model of T .*

PROOF. We may assume T is a set of $\forall\exists$ sentences. Consider a sentence

$$\varphi = \forall x \exists y \psi(x, y) \in T$$

where ψ is quantifier-free. We write φ as

$$\neg \exists x \neg \exists y \psi(x, y).$$

Suppose φ is not true in some $\mathfrak{M}(G)$ where G is generic for T . Then some $p \in G$ T -forces $\exists x \neg \exists y \psi(x, y)$, so

$$p \Vdash \neg \exists y \psi(c, y),$$

for some c . But p is consistent with T , so some $q \supseteq p$ must imply $\psi(c, d)$ for some d in C . Then

$$q \Vdash^* \exists y \psi(c, y),$$

a contradiction. We conclude that φ holds in every T -generic model. $\square$

To get an idea of the nature of T -generic models we shall look at some examples and introduce the notion of an existentially closed model.

8.10. EXAMPLE. Every generic linear ordering is isomorphic to the rationals. Every generic ordered field is real closed. Every generic field is algebraically closed. These examples can be verified directly using the definition of forcing.

8.11. DEFINITION. A model $\mathfrak{M}$ of T is *existentially closed* in T if every existential sentence φ of L_M which holds in some model of T extending $\mathfrak{M}$ holds in $\mathfrak{M}$.

It can be shown that the models described in Example 8.10 are existentially closed. The notion of an existentially closed model is a fruitful generalization of the notion of an algebraically closed field.

8.12. PROPOSITION. *If T is inductive, every model of T can be extended to an existentially closed model.*

The proof of this result is completely elementary, using only the fact that T is closed under unions of chains.

8.13. THEOREM. *If T is an inductive theory, every T -generic model is existentially closed in T .*

PROOF. Let M be T -generic, so M is the L -reduct of $\mathfrak{M}(G)$ for some generic G . Let $\exists x \varphi(x)$ hold in some model $\mathfrak{N} \models T$ extending $\mathfrak{M}$, where $\varphi(x)$ quantifier-free in L_c . Let $p \subseteq G$ and suppose the constant c does not occur in p or $\varphi(x)$. Using the diagram of $\mathfrak{N}$ we can find a condition $q \supseteq p$ such that

$$T \cup q \models \varphi(c).$$

By 8.7 and 8.9,

$$q \Vdash^* \exists x \varphi(x).$$

Therefore p cannot force $\neg \neg \neg \exists x \varphi(x)$. It follows that $G \Vdash \exists x \varphi(x)$, so $\exists x \varphi(x)$ holds in $\mathfrak{M}(G)$. $\square$

The treatment of forcing is continued in Chapter A.4, but in a more general context. That chapter has several basic results for the present special case. For example, Theorem 8.13 has the following converse.

8.14. THEOREM. *Let T be an inductive theory. If the class of all existentially closed models of T is elementary, then every countable existentially closed model of T is T -generic.*

Thus every countable real closed ordered field is a generic ordered field, and every countable algebraically closed field is a generic field. The case of groups has been extensively studied. There are countable existentially closed groups which are not generic (Chapter A.4).

Here is the eastern form of the omitting types theorem.

8.15. BASIC OMITTING TYPES THEOREM (MACINTYRE [1972b]). *Let T be an inductive theory, and let $\varphi_{mn}(x)$, $m, n < \omega$, be existential formulas. Suppose that for every condition p for T , each c in C , and each $m < \omega$, there is an $n < \omega$ such that*

$$T \cup p \cup \{\varphi_{mn}(c)\}$$

is consistent. Then T has a model $\mathfrak{M}$ which satisfies the infinite sentence $\bigwedge_m \forall x \bigvee_n \varphi_{mn}(x)$.

PROOF. We may choose a sequence of conditions $p_0 \subseteq p_1 \subseteq \dots$ such that

(1) $G = \bigcup_n p_n$ is generic.

(2) For each $m < \omega$ and each c in C , we have $p_k \Vdash \varphi_{mn}(c)$ for some $k, n < \omega$.

Then the reduct of $\mathfrak{M}(G)$ has the desired properties. $\square$

The proof of 8.15 shows that the model $\mathfrak{M}$ can be taken existentially closed in T .

8.16. EXAMPLE. Let T be an inductive theory containing the group axioms. Suppose that for each condition p for T and each $c \in C$ there is an n such that $p \cup \{nc = 0\}$ is consistent with T . Then T has a model which is a torsion group.

8.17. EXAMPLE. Let T be an inductive theory containing the ordered field axioms. Suppose that for each condition p for T and each $c \in C$ there is an n such that $p \cup \{c < n\}$ is consistent with T . Then T has an Archimedean model.

8.18. THEOREM (MACINTYRE [1972b]). *Suppose M is a group generated by $\{a_1, \dots, a_n\}$. If M is isomorphically embeddable in every existentially closed group, then the set E of equations in $a_1, \dots, a_n$ true in M is recursive.*

PROOF. Suppose E is not recursive. Let $\Phi(x)$ be the set of basic sentences not satisfied by $a_1, \dots, a_n$ in M . Then $\Phi(x)$ is not recursive. Since $\varphi \in \Phi$ iff $(\neg \varphi) \notin \Phi$, $\Phi(x)$ is not even recursively enumerable. We shall find an existentially closed group N such that

$$N \models \forall x \bigvee_{\varphi \in \Phi} \varphi(x).$$

M cannot be isomorphically embedded in such an N . Let p be a condition for group theory T and let $c_1, \dots, c_n \in C$. We claim that there is a $\varphi \in \Phi$ such that $p \cup \{\varphi(c)\}$ is a condition. For otherwise

$$\Phi(x) = \{\neg \psi(x) : T \cup p \models \psi(c)\}$$

and thus $\Phi(x)$ would be recursively enumerable. It follows by the basic omitting types theorem that the desired group N exists. $\square$

The T -generic models as defined here are necessarily countable. BARWISE and ROBINSON [1970] gave a more general definition which also allows uncountable T -generic models. We have presented Robinson's finite forcing. There is a parallel theory of infinite Robinson forcing, which is sketched briefly in Chapter A.4.

9. Infinite formulas and extra quantifiers

The restriction to first order logic is a severe limitation if we want to apply model theory to other parts of mathematics. Chapter A.1 gives several examples of concepts which are more naturally treated in stronger languages. The theorem of Lindström (in Chapter A.1) shows that first order logic is the only logic for which the compactness and Löwenheim–Skolem theorems hold. Nevertheless, there are two highly successful extensions of model theory to stronger logics. In model theory for infinitary logic we get by without the compactness theorem. In model theory with extra quantifiers we keep the compactness theorem but change the notion of a structure. We shall briefly discuss some of the methods which are available in these logics.

9.1. DEFINITION. Let κ be a regular cardinal. The logic $L_{\kappa\omega}$ is the set of formulas built up according to the following rules:

- (i) Every atomic formula of L , with variables x_α , $\alpha < \kappa$, is in $L_{\kappa\omega}$.
- (ii) If φ, ψ are in $L_{\kappa\omega}$, so are $\neg \varphi$, $\varphi \vee \psi$, and $\exists x \varphi$.
- (iii) If Φ is a set of formulas of $L_{\kappa\omega}$ of cardinality less than κ , then $\forall \Phi$ is in $L_{\kappa\omega}$.

We write $L_{\infty\omega} = \bigcup_{\kappa} L_{\kappa\omega}$, and for λ singular, $L_{\lambda\omega} = \bigcup_{\kappa < \lambda} L_{\kappa\omega}$.

9.2. EXAMPLE. $L_{\omega\omega}$ is ordinary first order logic. $L_{\omega_1\omega}$ is like first order logic but allows countable disjunctions.

The finite symbols $\wedge, \rightarrow, \leftrightarrow$, and $\forall$, and the infinite conjunction $\bigwedge$, may be introduced as abbreviations.

9.3. LEMMA. *Each formula of $L_{\kappa\omega}$ has fewer than κ subformulas.*

The notion of a subformula is defined in the natural way. (The separate definition of $L_{\kappa\omega}$ for singular κ is needed to make this lemma true.) The ω in $L_{\kappa\omega}$ indicates that finite quantifiers are allowed. More general languages $L_{\kappa\lambda}$ allow quantifiers over sets of fewer than λ variables.

In our discussion we shall concentrate on the two most important cases, $L_{\infty\omega}$ and $L_{\omega_1\omega}$.

In $L_{\infty\omega}$ a structure is completely determined up to isomorphism by its diagram

9.4. EXAMPLE. Given a structure $\mathfrak{M}$, we have $\mathfrak{N} \cong \mathfrak{M}$ if and only if $\mathfrak{N}$ satisfies the $L_{\infty\omega}$ sentence

$$\wedge D(\mathfrak{M}) \wedge \forall x \bigvee_{m \in M} x = m$$

$L_{\infty\omega}$ becomes more interesting when we work in the original language of $\mathfrak{M}$ without adding symbols for the elements of $\mathfrak{M}$.

9.5. EXAMPLE. The notion of an ω -saturated model is expressible by the following sentence of $L_{\infty\omega}$:

$$\bigwedge_{n < \omega} \bigwedge_{\Phi(x, y) \subseteq L} \left[\forall x \bigwedge_{\varphi_1, \dots, \varphi_n \in \Phi} \exists y (\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \exists y \bigwedge_{\varphi \in \Phi} \varphi \right]$$

9.6. EXAMPLE. Every well-ordering $\langle \alpha, < \rangle$ can be characterized up to isomorphism by a single sentence φ_α in $L_{\infty\omega}$ (with only the relation symbol $<$).

We first define, by induction on α , formulas $\psi_\alpha(x)$ stating that the set of predecessors of x has order type α :

$$\psi_0(x) = \neg \exists y y < x,$$

$$\psi_\alpha(x) = \bigwedge_{\beta < \alpha} \exists y (y < x \wedge \psi_\beta(y)) \wedge \forall y (y < x \rightarrow \bigvee_{\beta < \alpha} \psi_\beta(y))$$

Then we define φ_α by

$$\varphi_\alpha = (\text{linear order}) \wedge \bigwedge_{\beta < \alpha} \exists x \psi_\beta(x) \wedge \forall x \bigvee_{\beta < \alpha} \psi_\beta(x).$$

The notion of a well-ordering can be defined by the following sentence of $L_{\omega_1\omega_1}$:

$$(\text{linear order}) \wedge \neg (\exists x_0 x_1 x_2 \dots) \bigwedge_{n < \omega} x_{n+1} < x_n.$$

However, it *cannot* be defined by a sentence of $L_{\infty\omega}$.

9.7. THEOREM (LOPEZ-ESCOBAR [1966]). *Every sentence of $L_{\infty\omega}$ which has arbitrarily large well-ordered models has a nonwell-ordered model.*

The back and forth construction is useful in $L_{\infty\omega}$ and provides a characterization of $L_{\infty\omega}$ equivalence.

9.8. DEFINITION. $\mathfrak{M}$ and $\mathfrak{N}$ are $L_{\infty\omega}$ -equivalent, in symbols $\mathfrak{M} \equiv_{\infty\omega} \mathfrak{N}$, if they satisfy the same sentences of $L_{\infty\omega}$.

9.9. DEFINITION. A *partial isomorphism* $I : \mathfrak{M} \cong_p \mathfrak{N}$ is a relation I on the set of finite sequences (m, n) of elements of $M \times N$ such that:

- (i) $\emptyset I \emptyset$.
- (ii) If $m I n$, then $(\mathfrak{M}, m)$ and $(\mathfrak{N}, n)$ satisfy the same atomic sentences.
- (iii) If $m I n$ then for all $a \in M$ there exists $b \in N$ such that $(m, a) I (n, b)$, and vice versa.

9.10. THEOREM (KARP [1964]). $\mathfrak{M} \equiv_{\infty\omega} \mathfrak{N}$ if and only if $\mathfrak{M}$ and $\mathfrak{N}$ are partially isomorphic.

The following result is analogous to Lindström's Theorem (see Chapter A.1), and characterizes the logic $L_{\infty\omega}$.

9.11. THEOREM (BARWISE [1974]). $L_{\infty\omega}$ is the only logic closed under $\wedge, \neg, \exists$ which satisfies the nonwell-ordering Theorem 9.7 and Karp's Theorem 9.10.

The following examples show that in general $L_{\infty\omega}$ equivalence does not imply isomorphism.

9.12. EXAMPLE. By Theorem 9.10 the following are $L_{\infty\omega}$ equivalent, where X and Y are infinite sets.

$\langle \mathcal{P}(X), \subseteq \rangle$ and $\langle \mathcal{P}(Y), \subseteq \rangle$ where $\mathcal{P}(X)$ is the set of all subsets of X .

$G(X)$ and $G(Y)$ where $G(X)$ is the group freely generated by X .

$F[X]$ and $F[Y]$ where F is a field and $F[X]$ is the ring of polynomials over F in X .

Any two models of a complete ω -categorical theory in L .

Any two ω -saturated models of a complete theory in L .

BARWISE and EKLOF [1970] generalized the Ulm invariants to uncountable abelian groups and showed that two reduced torsion abelian groups have the same Ulm invariants if and only if they are $L_{\infty\omega}$ equivalent. For additional applications of partial isomorphisms see BARWISE [1973].

One trouble with the language $L_{\infty\omega}$ is that the formulas form a proper class rather than a set. Often one works with a set of formulas closed under subformulas. When we do this, the Downward Löwenheim-Skolem Theorem and the elementary chain theorem generalize to $L_{\infty\omega}$.

One more construction which is available in $L_{\infty\omega}$ is the notion of an Ehrenfeucht–Mostowski model, which is discussed in Chapter A.5.

The model theory for $L_{\omega_1\omega}$ is much more successful than that for $L_{\infty\omega}$. The key method is model-theoretic forcing, which we shall extend to $L_{\omega_1\omega}$. The method is equivalent to an earlier construction of Makkai called a consistency property (see KEISLER [1971]).

9.13. EXAMPLE. The notions of an Archimedean ordered field and of a torsion group are expressible by sentences in $L_{\omega_1\omega}$. So are the notions of a recursively saturated model, a prime model, and an ω -homogeneous model. In Section 6 we already used a sentence of $L_{\omega_1\omega}$ to state the omitting types theorem. The sentence $\forall x \bigvee_{n < \omega} x = \bar{n}$ holds in $\mathfrak{M}$ if and only if $\mathfrak{M}$ is an ω -model. From these examples, first order model theory leads quite naturally to $L_{\omega_1\omega}$.

Assume hereafter that L has countably many symbols.

Theorem 9.10 of Karp has the following sharper form for countable models.

9.14. THEOREM (SCOTT [1965]). *For every countable structure $\mathfrak{M}$ there is a sentence φ of $L_{\omega_1\omega}$ such that for all countable $\mathfrak{N}$,*

$$\mathfrak{N} \cong \mathfrak{M} \quad \text{iff} \quad \mathfrak{N} \models \varphi.$$

Let C be a countably infinite set of new constant symbols. We shall generalize model-theoretic forcing by replacing the set of sentences of L_C by a well behaved set of sentences of $(L_C)_{\omega_1\omega}$.

9.15. DEFINITION. By a *forcing base* we mean a countable set S of $(L_C)_{\omega_1\omega}$ sentences such that:

- (i) Each atomic sentence of L_C belongs to S .
- (ii) Each $\varphi \in S$ contains only finitely many $c \in C$.
- (iii) If $\psi(x)$ is a subformula of some $\varphi \in S$ and c is in C , then $\psi(c) \in S$.
- (iv) If $\varphi \in S$ and φ does not begin with $\neg$, then $(\neg \varphi) \in S$.

9.16. DEFINITION. A *forcing property* on S is a nonempty set P of consistent finite subsets $p \subseteq S$ such that

- (i) $p \in P$ and $q \subseteq p$ implies $q \in P$.
- (ii) If $p \models \exists x \varphi$ and $\varphi(c) \in S$, then $p \cup \{\varphi(d)\} \in P$ for some $d \in C$.
- (iii) If $\forall \Phi \in p$, then $p \cup \{\varphi\} \in P$ for some $\varphi \in \Phi$.

Using the elements $p \in P$ as conditions, the treatment of forcing goes exactly as before. The definition of forcing has a new clause for infinite disjunction,

$$p \Vdash \bigvee \Phi \quad \text{iff} \quad p \Vdash \varphi \quad \text{for some} \quad \varphi \in \Phi.$$

Robinson forcing as developed in Section 8 is the special case where the conditions $p \in P$ are finite sets of atomic and negated atomic sentences consistent with T . In the present more general setting the conditions may contain sentences with connectives and quantifiers. The definition of a forcing property insures that if $\varphi \in p$ then p weakly forces φ . By a *generic set* we mean a set $G \subseteq S$ such that each finite $p \subseteq G$ is a condition in P , and for each $\varphi \in S$ we have either $G \Vdash \varphi$ if $G \Vdash \neg \varphi$. Using the countability of S we see that every $p \in P$ can be extended to a generic set G .

9.17. GENERIC MODEL THEOREM. *For every generic set G there is model $\mathcal{M}(G)$ such that for all $\varphi \in S$,*

$$\mathcal{M}(G) \models \varphi \quad \text{iff} \quad G \Vdash \varphi.$$

The Generic Model Theorem is as useful in $L_{\omega_1\omega}$ as the compactness theorem is in first order logic. For example, the preservation theorems for substructures (Malitz), and homomorphic images (Lopez-Escobar), the Craig interpolation theorem (Lopez-Escobar), the two cardinal theorem from (κ, λ) to (ω_1, ω) (Keisler), the omitting types theorem, and the existence theorem for prime models can all be extended to $L_{\omega_1\omega}$ using the forcing construction.

The Generic Model Theorem can also be used to prove the following completeness theorem for $L_{\omega_1\omega}$.

9.18. Axioms for $L_{\omega_1\omega}$

All axiom schemes for L .

$\bigwedge \Phi \rightarrow \varphi$ for each $\varphi \in \Phi$.

9.19. Rules for $L_{\omega_1\omega}$

All rules of inference for L .

From $\{\psi \rightarrow \varphi : \varphi \in \Phi\}$ infer $\psi \rightarrow \bigwedge \Phi$.

We allow proofs of length less than ω_1 .

9.20. COMPLETENESS THEOREM FOR $L_{\omega_1\omega}$ (KARP [1964]). *A sentence φ of $L_{\omega_1\omega}$ is provable if and only if it is valid.*

PROOF. If φ is provable it is obviously valid. Suppose φ is not provable. Let S be a forcing base with $\varphi \in S$, and let P be the set of all finite $p \subseteq S$ such that p is formally consistent. From the axioms it follows that P is a forcing property. Since $\{\neg\varphi\}$ is a condition, $\neg\varphi$ has a generic model $\mathfrak{M}$, hence φ is not valid. $\square$

There is also an Upward Löwenheim–Skolem Theorem for $L_{\omega_1\omega}$. It is stated and proved for the special case of ω -logic in Chapter A.5.

One can do still more infinitary model theory by choosing the language more carefully using the notion of an admissible set (see Chapter A.7). The restriction of $L_{\omega_1\omega}$ to an admissible set A is denoted by L_A . When working with L_A one can bring in methods from generalized recursion theory. The most important result is the Barwise compactness theorem. For more about $L_{\omega_1\omega}$ and L_A see KEISLER [1971] and BARWISE [1975].

We conclude with a few words about extra quantifiers. Formally, the language $L(Q)$ is like first order logic but has an extra quantifier Q and the rule:

If φ is a formula, so is $Qx\varphi$.

These quantifiers were first studied by Mostowski. A structure for $L(Q)$ has the form $(\mathfrak{M}, q)$ where $\mathfrak{M}$ is a structure for L and q is a set of subsets of $\mathfrak{M}$. The definition of satisfaction has the extra clause

$$\mathfrak{M} \models Qx\varphi \quad \text{iff} \quad \{m \in M : \mathfrak{M} \models \varphi(m)\} \in q.$$

When we consider arbitrary structures, the model theory for $L(Q)$ is much like the model theory for L with few new difficulties. However, in the interesting applications of $L(Q)$ we restrict the class of models to reflect an intended interpretation of Q , and new problems arise.

One natural interpretation of Q is “there exist infinitely many”. For this interpretation, we consider only structures $(\mathfrak{M}, q)$ where q is the set of infinite subsets of $\mathfrak{M}$. This language is similar to ω -logic and is equivalent to a sublanguage of $L_{\omega_1\omega}$.

A second interpretation of Q is “there exist uncountably many”. We call this language $L(Q\omega_1)$. It is not part of $L_{\omega_1\omega}$ but has a very well behaved model theory. VAUGHT [1965] and FUHRKEN [1965] showed that the compactness theorem holds for countable theories, and the set of valid sentences is recursively enumerable. In KEISLER [1970] there is a completeness theorem with the simple set of axioms listed in Chapter A.1. The proof uses a form of the omitting types theorem, which also generalizes to $L(Q\omega_1)$. BRUCE [1975] has extended Robinson forcing to $L(Q\omega_1)$. It turns

out that the combined language $L_{\omega_1\omega}(Q\omega_1)$ also has a well behaved model theory.

Another successful interpretation of Q is aimed at studying topological models. In the logic $L(Q_{\text{open}})$ one considers models $(\mathfrak{M}, q)$ where q is the set of open sets of a topology on $\mathfrak{M}$. Thus $Qx\varphi(x)$ means “the set of x such that $\varphi(x)$ is open”. SGRO [1976a] has proved the compactness theorem for $L(Q_{\text{open}})$ using ultraproducts, and the completeness theorem with the following axioms:

- (1) Axioms for L .
- (2) $\forall x (\varphi \leftrightarrow \psi) \rightarrow (Qx\varphi \leftrightarrow Qx\psi)$.
- (3) $Qx\varphi(x) \leftrightarrow Qy\varphi(y)$.
- (4) $Qxx = x$.
- (5) $Qxx \neq x$.
- (6) $Qx\varphi \wedge Qx\psi \rightarrow Qx(\varphi \wedge \psi)$.
- (7) $\forall y Qx\varphi(x, y) \rightarrow Qx\exists y\varphi(x, y)$.

The last axiom says that “definable unions of open sets are open”. SGRO [1976b] and GARAVAGLIA [1975] have gone on to study stronger logics (the next step is quantifiers on two variables), and have applied $L(Q_{\text{open}})$ to topological groups.

References

- AX, J.
 [1968] The elementary theory of finite fields, *Ann. of Math.*, **88**, 239–271.
- BALDWIN, J.T. and A.H. LACHLAN
 [1971] On strongly minimal sets, *J. Symbolic Logic*, **36**, 79–96.
- BARWISE, J.
 [1973] Back and forth thru infinitary logic, in: *Studies in Model Theory*, edited by M Morley (Math. Assoc. Am., Buffalo, NY) pp. 5–34.
 [1974] Axioms for abstract model theory, *Ann. Math. Logic*, **7**, 221–265.
 [1975] *Admissible Sets and Structures* (Springer, Berlin).
- BARWISE, J. and P. EKLOF
 [1970] Infinitary properties of abelian groups, *Ann. Math. Logic*, **2**, 25–68.
- BARWISE, J. and A. ROBINSON
 [1970] Completing theories by forcing, *Ann. Math. Logic*, **2**, 119–142.
- BARWISE, J. and J. SCHLIPF
 [1976] Recursively saturated and resplendent models, to appear.
- BLUM, L.
 [1968] *Generalized Algebraic theories*, Thesis (M.I.T. Press, Cambridge, MA).
- BRUCE, K.
 [1975] Model-theoretic forcing and $L(\perp)$, Thesis, University of Wisconsin, Madison, WI.
- CHANG, C.C.
 [1965] A note on the two-cardinal problem, *Proc. Am. Math. Soc.*, **16**, 1148–1165.
 [1959] On unions of chains of models, *Proc. Am. Math. Soc.*, **10**, 120–127.

CHANG, C.C. and H. J. KEISLER

[1973] *Model Theory* (North-Holland, Amsterdam).

COBHAM, A.

[1962] Undecidability in group theory, *Notices Am. Math. Soc.*, **9**, 406.

CRAIG, W.

[1957] Three uses of the Herbrand–Gentzen theorem in relating model theory and proof theory, *J. Symbolic Logic*, **22**, 269–285.

ERDOS, P., L. GILLMAN and M. HENRIKSON

[1955] An isomorphism theorem for real closed fields, *Ann. of Math.*, Ser. 2, **61**, 542–554.

FUHRKEN, G.

[1965] Languages with added quantifier “there exist at least $\aleph_\alpha$ ”, in: *The Theory of Models*, edited by J.W. Addison, L. Henkin and A. Tarski (North-Holland, Amsterdam) pp. 121–131.

GARAVAGLIA, S.

[1975] Completeness for topological languages, Thesis, Yale University, New Haven, CT.

HAUSDORFF, F.

[1914] *Grundzüge der Mengenlehre* (Leipzig). [Reprinted by Chelsea, New York, 1955.]

HENKIN, L.

[1949] The completeness of the first-order functional calculus, *J. Symbolic Logic*, **14**, 159–166.

[1954] A generalization of the concept of ω -consistency, *J. Symbolic Logic*, **19**, 183–196.

JENSEN, R.

[1972] Fine structure of the constructible hierarchy, *Ann. Math. Logic*, **4**, 229–308.

JONSSON, B.

[1960] Homogeneous relational systems, *Math. Scand.*, **8**, 137–142.

KARP, C.

[1964] *Languages with Expressions of Infinite Length* (North-Holland, Amsterdam).

[1965] Finite-quantifier equivalence, in: *The Theory of Models*, edited by J.W. Addison, L. Henkin and A. Tarski (North-Holland, Amsterdam) pp. 407–412.

KEISLER, H.J.

[1970] Logic with the quantifier “there exist uncountably many”, *Ann. Math. Logic*, **1**, 1–93.

[1971] *Model Theory for Infinitary Logic* (North-Holland, Amsterdam).

[1973] Forcing and the omitting types theorem, in: *Studies in Model Theory*, edited by M. Morley (Math. Assoc. Am., Buffalo, NY) pp. 96–133.

[1976] Six classes of theories, *J. Austral. Math. Soc.*, to appear.

LACHLAN, A.

[1973] On the number of countable models of a countable superstable theory in: *Logic, Methodology and Philosophy of Science, IV*, edited by P. Suppes et al. (North-Holland, Amsterdam) pp. 45–56.

LOPEZ-ESCOBAR, E.

[1966] On definable well-orderings. *Fund. Math.*, **59**, 13–21.

ŁOŚ, J.

[1954] On the categoricity in power of elementary deductive systems and some related problems, *Colloq. Math.*, **3**, 58–62.

[1955] On the extending of models I, *Fund. Math.*, **42**, 38–54.

ŁOŚ, J. and R. SUSZKO

[1957] On the extending of models IV: infinite sums of models, *Fund. Math.*, **44**, 52–60.

LYNDON, R.

[1959] Properties preserved under homomorphisms, *Pacific J. Math.*, **9**, 143–154.

MACDOWELL, R. and E. SPECKER

[1961] Modelle der Arithmetik, in: *Infinitistic Methods* (Pergamon, London) pp. 257–263.

MACINTYRE, A.

[1972a] On algebraically closed groups, *Ann. of Math.*, **96**, 53–97.

[1972b] Omitting quantifier-free types in generic structures, *J. Symbolic Logic*, **37**, 512–520.

MALCEV, A.I.

[1971] *The Metamathematics of Algebraic Systems* (North-Holland, Amsterdam).

MORLEY, M.

[1965] Categoricity in power, *Trans. Am. Math. Soc.*, **114**, 514–538.

MORLEY, M., editor

[1973] *Studies in Model Theory* (Math. Assoc. Am., Buffalo, NY).

MORLEY, M. and R.L. VAUGHT

[1962] Homogeneous universal models, *Math. Scand.*, **11**, 37–57.

OREY, S.

[1956] On ω -consistency and related properties, *J. Symbolic Logic*, **21**, 246–252.

ROBINSON, A.

[1956a] *Complete Theories* (North-Holland, Amsterdam).

[1956b] A result on consistency and its application to the theory of definition, *Indag. Math.*, **18**, 47–58.

[1970] Forcing in model theory, 1st Nat. Alta Math., *Symposia Math.*, **5**, 69–82.

SACKS, G.

[1972] *Saturated Model Theory* (Benjamin, New York).

SCOTT, D.

[1965] Logic with denumerably long formulas and finite strings of quantifiers, in: *The Theory of Models*, edited by J.W. Addison, L. Henkin and A. Tarski (North-Holland, Amsterdam) pp. 329–341.

SGRO, J.

[1976a] Completeness theorems for topological models, *Ann. Math. Logic*, to appear.

[1976b] Completeness theorems for continuous functions and product topologies, *Israel J. Math.*, to appear.

SHELAH, S.

[1971] Stability, the finite cover property, and superstability, *Ann. Math. Logic*, **3**, 271–362.

[1974] Categoricity of uncountable theories, in: *Proceedings of the Tarski Symposium*, A.M.S. Proceedings of Symposia in Pure Mathematics, Vol. 25, pp. 187–203.

TARSKI, A.

[1954] Contributions to the theory of models I, II, *Indag. Math.*, **16**, 572–588.

TARSKI, A. and J.C.C. MCKINSEY

[1948] *A Decision Method for Elementary Algebra and Geometry* (Berkeley, Los Angeles, 2nd ed.).

TARSKI, A. and R.L. VAUGHT

[1957] Arithmetical extensions of relational systems, *Compositio Math.*, **13**, 81–102.

VAUGHT, R.L.

[1954] Applications of the Löwenheim–Skolem theorem to problems of completeness and decidability, *Indag. Math.*, **16**, 467–472.

[1961] Denumerable models of complete theories, in: *Infinitistic Methods* (Pergamon, London) pp. 303–321.

[1965] A Löwenheim–Skolem theorem for cardinals far apart, in: *The Theory of Models*, edited by J.W. Addison, L. Henkin and A. Tarski (North-Holland, Amsterdam) pp. 390–401.

Ultraproducts for Algebraists

PAUL C. EKLOF

Contents

Introduction	106
BASICS	
1. Filters	106
2. Reduced products	108
3. The fundamental theorem	111
4. Ultraproducts as functors	114
COMPACTNESS	
5. An ultraproduct version of the Compactness Theorem	118
6. Embedding theorems	120
7. Bounds in polynomial ideals	124
SATURATION	
8. Ultraproducts which are ω_1 -saturated	127
9. Ultraproducts of valued fields	132
10. Saturated models	134
References	135

Introduction

The ultraproduct construction is an algebraic operation whose importance derives from its model-theoretic properties. The algebraic character of the construction makes it a very attractive (though not essential) tool to employ in giving an account of applications of model theory to algebra.

This paper is a survey of the basic properties of ultraproducts and of some of their applications to algebra. The prerequisites for reading the paper are familiarity with the fundamental definitions of model-theory given in the previous chapters, and with the definitions of “category”, “functor”, and “natural transformation”. Moreover, since the applications to algebra are taken from such diverse areas as group theory, ring theory, algebraic geometry, universal algebra and algebraic number theory, we have found it necessary to assume an acquaintance with the algebraic notions and results used in the examples. (Usually we have given references for definitions and results not found in LANG [1971].) However, the reader may skip over a particular algebraic example without any loss of understanding of later material (except possibly of related algebraic examples).

The paper is divided into three parts. The first part, *Basics*, gives the definitions of ultrafilters and ultraproducts (as well as of a generalization of the ultraproduct called the reduced product) and proves the “fundamental theorem of ultraproducts”. In the last section of the first part we discuss the functorial properties of ultraproducts. The rest of the results are given in two parts, *Compactness* and *Saturation*, whose titles refer to the key model-theoretic properties of ultraproducts used in proving these results.

Some of the deepest applications of ultraproducts to algebra are only mentioned here, but references are given. Also, because the emphasis in this paper is on algebraic applications of ultraproducts, we have not discussed at all many interesting results about ultraproducts which do not fall under this heading. For more about ultraproducts we refer the reader to the excellent survey articles by KEISLER [1965] and CHANG [1967] and to the textbooks CHANG-KEISLER [1973] and BELL and SLOMSON [1969].

BASICS

1. Filters

If I is a non-empty set, a *filter over I* is a set D of subsets of I such that:

- (i) $\emptyset \notin D, I \in D$;

- (ii) if $X, Y \in D$, then $X \cap Y \in D$;
- (iii) if $X \in D$ and $X \subset Y \subset I$, then $Y \in D$.

For example, if Y is a non-empty subset of I , the set $\{X \subset I \mid Y \subset X\}$ is a filter over I , called the *principal filter* generated by Y ; we denote it by $\langle Y \rangle$. If I is finite, every filter over I is principal (generated by $\bigcap \{X \mid X \in D\}$). If I is infinite, an example of a non-principal filter over I is the *cofinite filter* $C = \{X \subset I \mid I - X \text{ is finite}\}$.

Notice that by (i) and (ii), a filter D over I has the *finite intersection property* (FIP), i.e., the intersection of any finite set of elements of D is non-empty. Obviously any subset of D also has FIP. Conversely, if S is a set of subsets of I which has the FIP, then S is a subset of a filter over I ; in fact

$$D = \{Y \subset I \mid X_1 \cap \cdots \cap X_n \subset Y \text{ for some } X_1, \dots, X_n \in S\}$$

is a filter containing S .

A filter D over I is called an *ultrafilter over I* if for every $X \subset I$, either $X \in D$ or $(I - X) \in D$.

1.1. PROPOSITION. *A filter over I is an ultrafilter if and only if it is a maximal filter over I .*

Proof. Suppose D is an ultrafilter over I and suppose E is a filter over I such that $D \subset E$ and $D \neq E$. Then $X \in E - D$ for some $X \subset I$. Since $X \notin D$ we have $I - X \in D$ by definition of an ultrafilter. But then $I - X \in E$, which is impossible since $\{X, I - X\} \subset E$ does not have the FIP. Conversely, suppose D is a maximal filter and let $X \subset I$ such that $X \notin D$. Then $D \cup \{I - X\}$ has FIP so it is a subset of a filter E . By the maximality of D , E must equal D and so $I - X \in D$. $\square$

An application of Zorn's Lemma yields the following.

1.2. COROLLARY. *If S is a set of subsets of I which has the finite intersection property, then S is contained in an ultrafilter over I .* $\square$

1.3. PROPOSITION. *If D is an ultrafilter over I , $X \in D$, and $X = Y_1 \cup \cdots \cup Y_n$, then for some i , $Y_i \in D$.*

Proof. If not, then by definition of ultrafilter, $I - Y_i$ is a member of D for all $i = 1, \dots, n$. But then by (ii) of the definition of a filter, $\emptyset = X \cap (I - Y_1) \cap \cdots \cap (I - Y_n)$ is a member of D , which contradicts (i). $\square$

A *principal ultrafilter* is an ultrafilter which is a principal filter. If D is a filter over I and $\{x\} \in D$ for some $x \in I$, then D is a principal ultrafilter over I generated by $\{x\}$; in fact, $Y \in D$ iff $Y \cap \{x\} \in D$ iff $\{x\} \subset Y$. Conversely, if D is a principal ultrafilter, then D must be generated by a singleton; for, otherwise, if D is generated by Y and there exists $\emptyset \neq Y' \subsetneq Y$, then the filter generated by Y' is a proper extension of D , contradicting 1.1. $\square$

1.4. PROPOSITION. *For any ultrafilter D over I , D is non-principal if and only if D contains C , the cofinite filter.*

PROOF. If D is a non-principal ultrafilter over I and $X = \{x_1, \dots, x_n\}$ is a finite subset of I , then by the above remarks $\{x_i\} \notin D$ for all $i = 1, \dots, n$. Hence $I - \{x_i\} \in D$ for all $i = 1, \dots, n$ so $\bigcap_{i=1}^n I - \{x_i\} = (I - X) \in D$. Therefore $C \subseteq D$. Conversely if $C \subseteq D$, then $\{x\} \notin D$ for all $x \in I$ (since $I - \{x\} \in C$), so by the remarks preceding the theorem, D is non-principal. $\square$

1.5. COROLLARY. *Let S be a set of subsets of I such that $X_1 \cap \dots \cap X_n$ is infinite for all $X_1, \dots, X_n \in S$. Then S is contained in a non-principal ultrafilter over I .*

PROOF. It follows from the hypothesis on S that $C \cup S$ has the FIP, so we can apply 1.2 and 1.4. $\square$

2. Reduced products

Let L be a first-order language; that is, L is a collection of relation, function, and constant symbols. We refer to 3.1 of Chapter A.1 for the definition of a model (or structure) $\mathfrak{A}$ for L . (When we talk about specific algebraic systems we will sometimes follow algebraic custom and denote the model $\mathfrak{A}$ by its universe A .) If Σ is a consistent set of sentences of L let $\mathcal{M}(\Sigma)$ denote the class of all models of Σ i.e. the class of all models $\mathfrak{A}$ for L such that every sentence of Σ is true in $\mathfrak{A}$, denoted $\mathfrak{A} \models \Sigma$. By an abuse of notation we shall write $\mathcal{M}(L)$ instead of $\mathcal{M}(\emptyset)$; thus $\mathcal{M}(L)$ is the class of all models for L .

If $\mathfrak{A}, \mathfrak{B} \in \mathcal{M}(L)$, a *homomorphism* η from $\mathfrak{A}$ to $\mathfrak{B}$ is a set function $\eta : A \rightarrow B$ which preserves all the relations, functions, and constants of L . For example, if $L = \{+, \leq, 0\}$ (where $+$ is a binary function symbol, $\leq$ is a

binary relation symbol and 0 is a constant symbol) then $\eta : \mathfrak{A} \rightarrow \mathfrak{B}$ is a homomorphism if and only if $\eta(0_{\mathfrak{A}}) = \eta(0_{\mathfrak{B}})$ and for all $a_1, a_2 \in A$

$$\eta(a_1 + a_2) = \eta(a_1) + \eta(a_2);$$

$$a_1 \leq a_2 \Rightarrow \eta(a_1) \leq \eta(a_2).$$

As usual, an *isomorphism* is a homomorphism which has an inverse homomorphism, and an *embedding* is a homomorphism which is an isomorphism onto its range.

If $\langle \mathfrak{A}_i : i \in I \rangle$ is a family of elements of $\mathcal{M}(L)$ indexed by a set I , denote by $\Pi_I \mathfrak{A}_i$ the direct product of the family; that is $\Pi_I \mathfrak{A}_i$ is the model for L whose universe is the direct product $\Pi_I A_i$ of the sets A_i and whose relations, functions and constants are defined "componentwise". For example, if $\mathfrak{A}_i = \langle A_i, +_i, \leq_i, 0_i \rangle$, then $\Pi_I \mathfrak{A}_i = \langle \Pi_I A_i, \tilde{+}, \tilde{\leq}, \tilde{0} \rangle$ where $\tilde{0}(i) = 0_i$ for all $i \in I$, and for any $f, g \in \Pi_I A_i$, $(f \tilde{+} g)(i) = f(i) +_i g(i)$; and $f \tilde{\leq} g$ iff $f(i) \leq_i g(i)$ for all $i \in I$.

If $\langle \mathfrak{A}_i : i \in I \rangle$ is a family indexed by I and X is a subset of I we shall understand by $\Pi_X \mathfrak{A}_i$ the direct product of the family $\langle \mathfrak{A}_i : i \in X \rangle$. Notice that if $Y \subset X \subset I$, the canonical projection $\pi_{XY} : \Pi_X \mathfrak{A}_i \rightarrow \Pi_Y \mathfrak{A}_i$ is a homomorphism.

Let D be a filter over a set I . Observe that if we define a partial ordering on D by $X \leq Y \Leftrightarrow X \supseteq Y$, then $(D, \leq)$ is a directed set (i.e. for any $X, Y \in D$ there exists $Z \in D$ such that $X \leq Z$ and $Y \leq Z$). If $\langle \mathfrak{A}_i : i \in I \rangle$ is a family of models for L indexed by I , the *reduced product* of $\langle \mathfrak{A}_i : i \in I \rangle$ modulo D , denoted $\Pi_D \mathfrak{A}_i$, is defined to be the direct limit (in $\mathcal{M}(L)$) of the directed system $\{\pi_{XY} : \Pi_X \mathfrak{A}_i \rightarrow \Pi_Y \mathfrak{A}_i \mid X, Y \in D, X \leq Y\}$. If D is an ultrafilter, $\Pi_D \mathfrak{A}_i$ is called the *ultraproduct* of $\langle \mathfrak{A}_i : i \in I \rangle$ modulo D . If $\mathfrak{A}_i = \mathfrak{A}$ for all $i \in I$, we write $\Pi_D \mathfrak{A}$ instead of $\Pi_D \mathfrak{A}_i$ and call it the *ultrapower* of $\mathfrak{A}$ modulo D .

Although the shortest approach to the definition of reduced products is via the notion of direct limit, this approach is perhaps misleading since it is the concrete construction of the direct limit rather than its universal mapping properties which will be of importance in the sequel. So let us describe the structure of $\Pi_D \mathfrak{A}_i$ more explicitly. The following description of the reduced product follows easily from the usual construction of direct limit, given the observation that for every $X \in D$ the projection π_{IX} is surjective, so that every element of the direct limit is represented by an element of $\Pi_I \mathfrak{A}_i$. Those readers who are not comfortable with the notion of direct limits may take the following as the definition of reduced products.

Define an equivalence relation $=_D$ on $\Pi_I \mathfrak{A}_i$ as follows: If $f, g \in \Pi_I \mathfrak{A}_i$,

then $f =_D g$ if and only if $\pi_{IX}(f) = \pi_{IX}(g)$ for some $X \in D$ i.e. $f =_D g$ if and only if $\{i \in I \mid f(i) = g(i)\}$ is an element of D . The universe of $\Pi_D \mathfrak{A}_i$ is the set $\Pi_D A_i$ of equivalence classes of elements of $\Pi_I A_i$. Denote the equivalence class of $f \in \Pi_I A_i$ by f_D .

The relations on $\Pi_D \mathfrak{A}_i$ are defined by the condition that a relation holds between elements of $\Pi_D \mathfrak{A}_i$ if and only if it holds on a set of components which belongs to D ; similarly for functions. For example, if $\mathfrak{A}_i = \langle A_i, +_i, \leq_i, 0_i \rangle$ and $f_D, g_D, h_D \in \Pi_D A_i$, then $f_D \leq g_D$ in $\Pi_D \mathfrak{A}_i$ if and only if $\{i \in I \mid f(i) \leq_i g(i)\} \in D$. (Equivalently, $f_D \leq g_D$ if and only if there exists $X \in D$ such that $\pi_{IX}(f) \leq \pi_{IX}(g)$ in $\Pi_X \mathfrak{A}_i$.) Similarly, $f_D + g_D = h_D$ in $\Pi_D \mathfrak{A}_i$ if and only if $\{i \in I \mid f(i) + g(i) = h(i)\} \in D$. And the interpretation of 0 in $\Pi_D \mathfrak{A}_i$ is $\tilde{0}_D$ where $\{i \in I \mid \tilde{0}(i) = 0_i\} \in D$. It is easy to verify, using the properties of filters, that $\leq$, $+$, and 0 on $\Pi_D \mathfrak{A}_i$ are well-defined.

The following lemma justifies the similarity of our notation for direct products and reduced products. It is an immediate consequence of the fact that the directed set $(\langle X \rangle, \leq)$ has X as a largest element.

2.1. LEMMA. *If $\langle X \rangle$ is the principal filter over I generated by X , then the reduced product of $\langle \mathfrak{A}_i : i \in I \rangle$ modulo $\langle X \rangle$ is isomorphic to the direct product of $\langle \mathfrak{A}_i : i \in X \rangle$ (i.e. $\Pi_{\langle X \rangle} A_i \cong \Pi_X A_i$).*

It is ultraproducts rather than reduced products in general that are of most interest to logicians since ultraproducts preserve logical properties of the family $\langle \mathfrak{A}_i : i \in I \rangle$ (in a sense which is made precise in the main theorem of the next section). But before proceeding to that, let us mention that in the case when the models are division rings, an alternate construction of the reduced product may be given.

Let $\langle R_i : i \in I \rangle$ be a family of division rings. For any $f \in \Pi_I R_i$, let $Z(f) = \{i \in I \mid f(i) = 0\}$. Notice that for any $f, g \in \Pi_I R_i$, we have $Z(f) \subseteq Z(g)$ if and only if there exists $h_1 \in \Pi_I R_i$ such that $h_1 f = g$ if and only if there exists $h_2 \in \Pi_I R_i$ such that $f h_2 = g$. (Here we use the fact that the R_i 's are division rings.) It follows that every (left or right) ideal of $\Pi_I R_i$ is two-sided. If N is a subset of $\Pi_I R_i$, let $Z(N) = \{Z(f) : f \in N\}$.

2.2. THEOREM (KOCHEN [1961]). *Let $\langle R_i : i \in I \rangle$ be a family of division rings. If N is an ideal of $\Pi_I R_i$, then $Z(N)$ is a filter over I . The mapping, Z , which assigns N to $Z(N)$ is a one-one inclusion-preserving correspondence between proper ideals of N and filters over I . Under this mapping, principal ideals correspond to principal filters and maximal ideals correspond to*

ultrafilters. Moreover, for any ideal N of $\prod_i R_i$, the quotient ring $\prod_i R_i/N$ is isomorphic to the reduced product $\prod_{Z(N)} R_i$.

PROOF. If S is a subset of I , let $\bar{S} \in \prod_i R_i$ denote the "characteristic function" of S i.e. $\bar{S} : I \rightarrow \{0, 1\} \subset R$ such that $\bar{S}(x) = 0$ if and only if $x \in S$. Notice that if N is an ideal of $\prod_i R_i$ and $f \in \prod_i R_i$, then $f \in N$ if and only if $\overline{Z(f)} \in N$. It follows that for any $f, g \in N$, $Z(f) \cap Z(g) \in Z(N)$, since

$$Z(f) \cap Z(g) = \overline{Z(\overline{Z(f)} + \overline{Z(g)})} + \overline{Z(f)} \overline{Z(g)}.$$

(A simpler expression is possible if none of the R_i have characteristic 2.) Thus $Z(N)$ satisfies (ii) of the definition of a filter; parts (i) and (iii) of the definition follow easily from the definition of $Z(N)$ and the remarks preceding the theorem. Hence $Z(N)$ is a filter.

If D is a filter over I let $N_D = \{f \in \prod_i R_i \mid Z(f) \in D\}$; then N is an ideal since $Z(f - g) \supseteq Z(f) \cap Z(g)$ and $Z(fg) \supseteq Z(f)$; N is proper since $\emptyset \notin D$. The mapping which takes D to N_D is inverse to the mapping Z and hence Z is a one-one correspondence between ideals of $\prod_i R_i$ and filters over I . Since Z is clearly inclusion preserving, maximal ideals correspond to maximal filters i.e. ultrafilters (see Proposition 1.1). It is also easy to verify that the ideal N is generated by f if and only if $Z(N)$ is generated by $Z(f)$. Finally, the function which takes the coset $f + N$ in $\prod_i R_i/N$ to $f_D \in \prod_{Z(N)} R_i$ is an isomorphism of rings. $\square$

2.3. COROLLARY. *If $\langle R_i : i \in I \rangle$ is a family of division rings and N is a prime ideal of $\prod_i R_i$, then N is a maximal ideal and $\prod_i R_i/N$ is a division ring.*

PROOF. To prove that N is maximal, it suffices to prove $Z(N)$ is an ultrafilter. Let $X \subset I$. If $X \notin Z(N)$ and $I - X \notin Z(N)$, then $\bar{X}$ and $\overline{I - X}$ are not in N . But $\bar{X}(\overline{I - X}) = 0 \in N$, a contradiction. Therefore $Z(N)$ is an ultrafilter. To see that $\prod_i R_i/N$ is a division ring, let $f \in \prod_i R_i$ such that $f \notin N$. Then $Z(f) \notin Z(N)$ so $I - Z(f) \in Z(N)$. If $g \in \prod_i R_i$ such that $g(i) = f(i)^{-1}$ for all $i \in I - Z(N)$, then $\{i \in I \mid g(i)f(i) = 1\} = I - Z(f) \in N$. Therefore by the remarks preceding Theorem 2.2, $1 - gf \in N$, i.e. f is a unit in $\prod_i R_i/N$. $\square$

3. The fundamental theorem

As a result of Corollary 2.3 we know that an ultraproduct of division rings is a division ring (while a reduced product of division rings which is

not an ultraproduct will *not* be a division ring). This is a special case of the fundamental theorem of ultraproducts which says that elementary properties of the family $\langle \mathfrak{A}_i : i \in I \rangle$ are preserved under ultraproducts. More precisely, the fundamental theorem, or Łoś' Theorem, is the following.

3.1. THEOREM (ŁOŚ [1955]). *Let $\langle \mathfrak{A}_i : i \in I \rangle$ be a family of models for L and let D be an ultrafilter over I . Then for any formula $\varphi(x_1, \dots, x_n)$ of L and any elements $g^1, \dots, g^n$ of $\prod_i \mathfrak{A}_i$,*

$$\prod_D \mathfrak{A}_i \models \varphi [g_D^1 \cdots g_D^n]$$

if and only if

$$\{i \in I \mid \mathfrak{A}_i \models \varphi [g^1(i) \cdots g^n(i)]\} \in D.$$

Before proving the fundamental theorem, let us consider some consequences of it. For the case when φ has no free variables we obtain the following.

3.2. COROLLARY. *For any ultraproduct $\prod_D \mathfrak{A}_i$ and any sentence φ , $\prod_D \mathfrak{A}_i \models \varphi$ if and only if $\{i \in I \mid \mathfrak{A}_i \models \varphi\} \in D$.*

3.3. COROLLARY. *If $\mathfrak{A}_i$ is in $\mathcal{M}(\Sigma)$ for each $i \in I$, then the ultraproduct $\prod_D \mathfrak{A}_i$ is in $\mathcal{M}(\Sigma)$.*

A subclass of $\mathcal{M}(L)$ which is of the form $\mathcal{M}(\Sigma)$ for some set of sentences Σ of L is called (*first-order*) *axiomatizable*, or *elementary*. Corollary 3.3 says that any axiomatizable class is closed under ultraproducts. For example, an ultraproduct of groups (semigroups; rings; commutative rings; fields; algebraically closed fields; division rings; formally real fields; real closed fields; Lie algebras; Boolean algebras; etc.) is a group (semigroup; ring; commutative ring; field; algebraically closed field; division ring; formally real field; real closed field; Lie algebra; Boolean algebra; etc.) because the class in question is axiomatizable. Proving that a class is not closed under ultraproducts is a useful method of proving that a class is not axiomatizable. We give an example. A different proof is given in 2.3 of Chapter A.1. It is instructive to compare the two proofs.

3.4. COROLLARY. *Let $L = \{+, 0\}$ be the language of abelian groups (i.e. L has a binary function symbol, $+$, and a constant symbol 0). The class of torsion abelian groups is not first-order axiomatizable.*

PROOF. It suffices to produce an ultraproduct of torsion abelian groups which is not torsion. Let $I = \omega$ and let A_n be the cyclic group of order $n + 1$ for each $n \in I$. We claim that if D is a non-principal ultrafilter over I , then $\Pi_D A_n$ is not torsion. Let $f \in \Pi_I A_n$ be such that $f(n)$ has order $n + 1$ for each $n \in I$. For any $m > 0$, if $\varphi_m(x)$ is the formula

$$(x + x + \cdots + x = 0)$$

(where x occurs m times), then by 3.1, $\Pi_D A_n \not\models \varphi_m[f_D]$ since

$$\{n \in I \mid A_n \models \varphi_m[f(n)]\}$$

is a finite set and hence is not in D by 1.4. Therefore f_D is not of finite order. (Instead of appealing to 3.1 we could verify directly from the definitions that $mf_D \neq 0$ in $\Pi_D A_n$ for any $m \neq 0$.) Hence $\Pi_D A_n$ is not torsion. $\square$

This method of proving that a class is not axiomatizable will not always work since—as we shall see in Section 4—there are classes closed under ultraproducts which are not axiomatizable. See Section 5 for an ultraproduct method of proving that a class is not finitely axiomatizable. Now let us prove 3.1.

PROOF OF THEOREM 3.1. For the sake of concreteness we shall prove the theorem for our standard example, $\mathfrak{A}_i = \langle A_i, +, \leq, 0_i \rangle$, but the argument is perfectly general. The proof is by induction on the formula φ . Consider first the simplest kinds of atomic formulas: $x_1 \leq x_2$; $x_1 + x_2 = x_3$; or $x_1 = 0$. If φ is one of these, then the result follows from the definition of the ultraproduct.

The most general types of atomic formulas are $t_1 \leq t_2$ and $t_1 = t_2$ where t_1 and t_2 are terms built up from the function symbol $+$ and the constant symbol 0 [e.g. $t_1 = ((x_1 + x_2) + ((0 + x_3) + x_1)) + ((x_4 + x_2) + 0)$]. In this case, the desired result follows from the first case above once we prove, by induction on the construction of a term $t(x_1 \cdots x_n)$, that $t_{\Pi_D \mathfrak{A}_i}[g^1_D \cdots g^n_D] = h_D$ if and only if $\{i \in I \mid t_{\mathfrak{A}_i}[g^1(i) \cdots g^n(i)] = h(i)\} \in D$. We leave the details to the reader: the initial cases ($t = x_{i_1} + x_{i_2}$; $t = x_i$; or $t = 0$) follow from the definition of the ultraproduct. (See 3.7 in Chapter A.1 for the definition of $t_{\mathfrak{A}_i}$, there written $t^{\mathfrak{A}_i}$.)

Now suppose $\varphi = \neg \psi(x_1 \cdots x_n)$ and suppose the theorem proved for ψ . Then

$$\begin{aligned}
\Pi_D \mathfrak{A}_i \models \varphi [g_D^1 \cdots g_D^n] &\Leftrightarrow \Pi_D \mathfrak{A}_i \not\models \psi [g_D^1 \cdots g_D^n] \\
&\Leftrightarrow \{i \in I \mid \mathfrak{A}_i \models \psi [g^1(i) \cdots g^n(i)]\} \notin D \\
&\Leftrightarrow \{i \in I \mid \mathfrak{A}_i \not\models \psi [g^1(i) \cdots g^n(i)]\} \in D \\
&\Leftrightarrow \{i \in I \mid \mathfrak{A}_i \models \varphi [g^1(i) \cdots g^n(i)]\} \in D
\end{aligned}$$

(The next to last equivalence uses the fact that D is an ultrafilter, not simply a filter.) If $\varphi = \psi_1 \wedge \psi_2$, and the theorem is assumed for ψ_1 and ψ_2 , a similar argument proves the result for φ ; here, the key fact is that for any filter D , $X \cap Y \in D$ if and only if $X \in D$ and $Y \in D$.

Finally, if $\varphi = \exists x_0 \psi(x_1 \cdots x_n)$, then $\Pi_D \mathfrak{A}_i \models \varphi [g_D^1 \cdots g_D^n] \Leftrightarrow$ there exists $g^0 \in \Pi_I \mathfrak{A}_i$ such that $\Pi_D \mathfrak{A}_i \models \psi [g_D^0, g_D^1, \dots, g_D^n] \Leftrightarrow$ there exists $g^0 \in \Pi_I \mathfrak{A}_i$ such that

$$\begin{aligned}
\{i \in I \mid \mathfrak{A}_i \models \psi [g^0(i), g^1(i), \dots, g^n(i)]\} &\in D \Rightarrow \\
\Rightarrow \{i \in I \mid \mathfrak{A}_i \models \varphi [g^1(i) \cdots g^n(i)]\} &\in D.
\end{aligned}$$

Conversely, if $\{i \in I \mid \mathfrak{A}_i \models \varphi [g^1(i) \cdots g^n(i)]\} = X \in D$, then there exists $g^0 \in \Pi_I \mathfrak{A}_i$ such that for every $i \in X$, $\mathfrak{A}_i \models \psi [g^0(i), g^1(i), \dots, g^n(i)]$; hence $\{i \in I \mid \mathfrak{A}_i \models \psi [g^0(i), g^1(i), \dots, g^n(i)]\} \in D$. $\square$

Because of the importance of the fundamental theorem, from now on we shall confine our attention to ultraproducts (and ultrapowers) rather than arbitrary reduced products.

4. Ultraproducts as functors

Throughout the paper we shall assume that all the classes of models we consider are closed under isomorphism. If $\mathcal{A}$ is a subclass of $\mathcal{M}(\mathbf{L})$, we shall also denote by $\mathcal{A}$ the *category* whose objects are the elements of $\mathcal{A}$ and whose morphisms are all the homomorphisms between elements of $\mathcal{A}$. We shall also consider the category $\mathcal{A}^I$, whose objects are the indexed families $\langle \mathfrak{A}_i : i \in I \rangle$ of objects of $\mathcal{A}$ and whose morphisms from $\langle \mathfrak{A}_i : i \in I \rangle$ to $\langle \mathfrak{B}_i : i \in I \rangle$ are the indexed families $\langle \eta_i : i \in I \rangle$ of homomorphisms $\eta_i : \mathfrak{A}_i \rightarrow \mathfrak{B}_i$. Since these are the only categories we consider, we shall freely interchange the words “class” and “category” in referring to $\mathcal{A}$ or $\mathcal{A}^I$.

If $\langle \eta_i : i \in I \rangle$ is a family of homomorphisms $\eta_i : \mathfrak{A}_i \rightarrow \mathfrak{B}_i$, let $\Pi_D \eta_i : \Pi_D \mathfrak{A}_i \rightarrow \Pi_D \mathfrak{B}_i$ be the function defined by $(\Pi_D \eta_i)(f_D) = g_D$, where $g(i) = \eta_i(f(i))$. It is easy to check that $\Pi_D \eta_i$ is a well-defined homomorphism called the *ultraproduct of the η_i modulo D* .

If $\eta_i = \eta : \mathfrak{A} \rightarrow \mathfrak{B}$ for all $i \in I$, then $\Pi_D \eta_i$ is denoted by $\Pi_D \eta$ and called

the *ultrapower of η modulo D* ; it is a homomorphism from $\Pi_D \mathfrak{A}$ to $\Pi_D \mathfrak{B}$. It is now a routine exercise in the definitions to verify the following result. The notion of *elementary embedding* is defined in Chapter A.2.

4.1. THEOREM. *If D is an ultrafilter over I and $\mathcal{A}$ is a subclass of $\mathcal{M}(L)$ closed under ultrapowers (resp. ultraproducts), then the ultrapower (resp. ultraproduct) Π_D is a functor from $\mathcal{A}$ to $\mathcal{A}$ (resp. from $\mathcal{A}^1$ to $\mathcal{A}$).*

4.2. THEOREM. *The ultrapower functor on $\mathcal{A}$ preserves embeddings and elementary embeddings. Similarly the ultraproduct functor takes a family $\langle \eta_i : i \in I \rangle$ of embeddings (resp. elementary embeddings) to an embedding (resp. elementary embedding).*

PROOF. It suffices to prove the result for ultraproducts. Now by definition $\eta_i : \mathfrak{A}_i \rightarrow \mathfrak{B}_i$ is an embedding iff $\eta_i : \mathfrak{A}_i \rightarrow \text{ran } \eta_i$ is an isomorphism. Thus if $\langle \eta_i : i \in I \rangle$ is a family of embeddings, $\Pi_D \eta_i$ is an embedding because functors preserve isomorphisms and the range of $\Pi_D \eta_i = \Pi_D \text{ran } \eta_i$. For the case of elementary embeddings we appeal to the fundamental theorem (3.1). Suppose $\varphi(x_1 \cdots x_n)$ is a formula of L and $g^1_b, \dots, g^n_b \in \Pi_D \mathfrak{A}_i$. Then

$$\begin{aligned} \Pi_D \mathfrak{A}_i \models \varphi[g^1_b \cdots g^n_b] &\Leftrightarrow \{i \in I \mid \mathfrak{A}_i \models \varphi[g^1(i) \cdots g^n(i)]\} \in D \\ &\Leftrightarrow \{i \in I \mid \mathfrak{B}_i \models \varphi[\eta_i(g^1(i)) \cdots \eta_i(g^n(i))]\} \in D \\ &\Leftrightarrow \Pi_D \mathfrak{B}_i \models \varphi[(\Pi_D \eta_i)(g^1_b) \cdots (\Pi_D \eta_i)(g^n_b)]. \quad \square \end{aligned}$$

One useful aspect of the ultraproduct construction is that—for a fixed ultrafilter—it provides a uniform way of defining functors on different categories. In order to give a formal expression of this uniformity we need a notion of “forgetful functor”. Let L, L' be first-order languages such that $L \subset L'$. Recall that a model for L' is a pair $\mathfrak{A}' = \langle A', \mathcal{J}' \rangle$ where $\mathcal{J}'$ assigns an interpretation of each symbol of L' . If $\mathfrak{A}'$ is a model for L' , let $R_{L,L}(\mathfrak{A}')$ be the model $\mathfrak{A} = \langle A', \mathcal{J} \rangle$ for L where $\mathcal{J}$ is the restriction of $\mathcal{J}'$ to the symbols of L . $R_{L,L}(\mathfrak{A}')$ is called the *reduct* of $\mathfrak{A}'$ to L . If $\eta : \mathfrak{A}' \rightarrow \mathfrak{B}'$ is a homomorphism of models for L' , $R_{L,L}(\eta)$ is the same set function η regarded as a homomorphism of $R_{L,L}(\mathfrak{A}')$ to $R_{L,L}(\mathfrak{B}')$. It is easily seen that $R_{L,L}$ is a functor from $\mathcal{M}(L')$ to $\mathcal{M}(L)$ called the *forgetful functor*. (We shall drop the subscripts on R where, in context, there is no ambiguity.) For example, if L is the empty set of symbols and $L \subset L'$, then $\mathcal{M}(L)$ is the category of sets and $R_{L,L}$ is the familiar underlying set functor from $\mathcal{M}(L')$ to $\mathcal{M}(L)$.

If $R_{L,L}$ takes the subclass $\mathcal{A}'$ of $\mathcal{M}(L)$ to the subclass $\mathcal{A}$ of $\mathcal{M}(L)$ we shall also denote by $R_{L,L}$ the restriction of $R_{L,L}$ to $\mathcal{A}$ and call it the *forgetful functor from $\mathcal{A}'$ to $\mathcal{A}$* . For example there is a forgetful functor $R_{L,L}$ from the class of ordered abelian groups to the class of abelian groups. (Here $L = \{+, 0\}$ and $L' = \{+, \leq, 0\}$.)

The next result is now an easy consequence of the definitions.

4.3. THEOREM. *Let D be an ultrafilter over I and let L and L' be first-order languages such that $L \subset L'$. Then the following diagrams (for the ultrapower and ultraproduct respectively) are commutative.*

$$\begin{array}{ccc} \mathcal{M}(L') & \xrightarrow{R_{L,L}} & \mathcal{M}(L) \\ \downarrow \Pi_D & & \downarrow \Pi_D \\ \mathcal{M}(L') & \xrightarrow{R_{L,L}} & \mathcal{M}(L) \end{array} \qquad \begin{array}{ccc} \mathcal{M}(L')^I & \xrightarrow{R_{L,L}^I} & \mathcal{M}(L)^I \\ \downarrow \Pi_D & & \downarrow \Pi_D \\ \mathcal{M}(L') & \xrightarrow{R_{L,L}} & \mathcal{M}(L) \end{array}$$

Theorem 4.3 is useful in proving that certain classes are closed under ultraproducts, even when we do not know if the class is axiomatizable. Let us say that a class $\mathcal{A} \subset \mathcal{M}(L)$ is *pseudo-elementary* if there is a forgetful functor $R = R_{L,L}$ such that $\mathcal{A}$ is the image under R of an elementary (i.e. axiomatizable) class $\mathcal{A}' \subset \mathcal{M}(L')$.

4.4. COROLLARY. *A pseudo-elementary class is closed under ultraproducts.*

PROOF. Maintaining the notation of the definition, let us prove that for any family $\{\mathfrak{A}_i : i \in I\}$ in $\mathcal{A}$, $\Pi_D \mathfrak{A}_i$ is in $\mathcal{A}$. By hypothesis, each $\mathfrak{A}_i$ is of the form $R(\mathfrak{A}'_i)$ for some $\mathfrak{A}'_i$ in $\mathcal{A}'$. But then by Corollary 3.3 and Theorem 4.3 we have

$$\Pi_D \mathfrak{A}_i = \Pi_D R(\mathfrak{A}'_i) = R(\Pi_D \mathfrak{A}'_i) \in R(\mathcal{A}') \subset \mathcal{A}. \quad \square$$

4.5. THEOREM. *Let $n \in \omega$. If $\mathcal{A}$ is the class of all groups which are isomorphic to $GL(n, F)$ for some field F , then $\mathcal{A}$ is closed under ultraproducts.*

PROOF. Here we use $GL(n, F)$ to denote the group, under multiplication, of the invertible $n \times n$ matrices over F . By 4.4 it suffices to prove that $\mathcal{A}$ is pseudo-elementary. Expand the language $L = \{\cdot, e\}$ of groups to $L' = \{\cdot, e, +, *, 0, 1, \pi_{ij}\}$ where $+, *$ are binary function symbols, 0 and 1 are constant symbols, and π_{ij} , $1 \leq i, j \leq n$, are unary function symbols. Let $\mathcal{A}'$

be the class of all models $\mathfrak{A} = \langle A, \cdot, e, +, *, 0, 1, \pi_{ij} \rangle$ for L' satisfying the following properties (which are easily seen to be expressible as sentences in L'):

- (i) two elements a_1, a_2 of A are equal if and only if $\pi_{ij}(a_1) = \pi_{ij}(a_2)$ for all i, j (hence elements of A "are" $n \times n$ matrices);
- (ii) the union F of the ranges of the π_{ij} forms a field with respect to $+, *, 0$, and 1 ;
- (iii) the "matrix" e is the identity matrix;
- (iv) the operation $\cdot$ is matrix multiplication; and
- (v) the elements of A are precisely the $n \times n$ matrices over F which are invertible.

Then $\mathcal{A}$ is the image of $\mathcal{A}'$ under the forgetful functor. $\square$

The class $\mathcal{A}$ in the above theorem is known not to be axiomatizable. (See SABBAGH [1969]; the proof is given for $n = 1$, but it generalizes to arbitrary n .) It is an open problem whether the class in the next theorem is elementary or not.

4.6. THEOREM (Sabbagh). *The class of primitive rings is closed under ultraproducts.*

PROOF. For our purposes, the most convenient definition of a primitive ring is that R is primitive if and only if there is a maximal regular right ideal ρ in R such that $(\rho : R) = (0)$ (see HERSTEIN [1968], p. 40). With this definition it is not hard to see that the class of primitive rings is pseudo-elementary. $\square$

We conclude this section with one other useful result about ultrapowers.

4.7. THEOREM. *Let D be an ultrafilter over a set I . There is a natural transformation $d : I \rightarrow \Pi_D$, from the identity functor on $\mathcal{M}(L)$ to the ultrapower functor on $\mathcal{M}(L)$ such that for each $\mathfrak{A}$ in $\mathcal{M}(L)$, $d(\mathfrak{A})$ is an elementary embedding. Moreover, for any expansion L' of L we have $R_{L'L}d = dR_{L'L}$.*

PROOF. For any $\mathfrak{A}$ in $\mathcal{M}(L)$ let $d(\mathfrak{A}) : \mathfrak{A} \rightarrow \Pi_D \mathfrak{A}$ be defined by $d(a) = \tilde{a}_D$ where $\tilde{a} : I \rightarrow \mathfrak{A}$ is the constant function with value a . That $d(\mathfrak{A})$ is an elementary embedding follows from the fundamental theorem, 3.1, since

$$\begin{aligned} \Pi_D \mathfrak{A} \models \varphi[d(a_1) \cdots d(a_n)] &\Leftrightarrow \{i \in I \mid \mathfrak{A}_i = \mathfrak{A} \models \varphi[a_1 \cdots a_n]\} \in D \\ &\Leftrightarrow \mathfrak{A} \models \varphi[a_1 \cdots a_n]. \end{aligned}$$

We leave to the reader the easy verification that d is a natural transformation (i.e. $d(\mathfrak{B}) \circ f = \Pi_D(f) \circ d(\mathfrak{A})$ for any $f: \mathfrak{A} \rightarrow \mathfrak{B}$) and that $R_{L^L}d = dR_{L^L}$. $\square$

COMPACTNESS

5. An ultraproduct version of the Compactness Theorem

The fundamental theorem implies that for any family $\langle \mathfrak{A}_i : i \in I \rangle$ and any ultrafilter D , if each $\mathfrak{A}_i$ satisfies a set of first-order sentences Σ , then $\Pi_D \mathfrak{A}_i$ also satisfies Σ . The content of the next theorem (which is an easy corollary of the fundamental theorem) is that for certain ultrafilters D , the ultraproduct $\Pi_D \mathfrak{A}_i$ may satisfy a set of first-order properties Σ though no $\mathfrak{A}_i$ is a model of Σ .

5.1. THEOREM. *Let $\langle \mathfrak{A}_i : i \in I \rangle$ be an indexed family of models for L and let Σ be a set of sentences of L .*

(i) *If for every sentence φ of Σ , $\{i \in I \mid \mathfrak{A}_i \models \varphi\}$ is cofinite, then for any non-principal ultrafilter D over I , $\Pi_D \mathfrak{A}_i$ is a model of Σ .*

(ii) *If for every finite subset $\{\varphi_1, \dots, \varphi_n\}$ of Σ , $\{i \in I \mid \mathfrak{A}_i \models \varphi_1 \wedge \dots \wedge \varphi_n\}$ is non-empty, then there exists an ultrafilter D over I such that $\Pi_D \mathfrak{A}_i$ is a model of Σ .*

PROOF. (i) By Proposition 1.4, if D is non-principal, then $\{i \in I \mid \mathfrak{A}_i \models \varphi\}$ is in D , for every $\varphi \in \Sigma$, and therefore, by Corollary 3.2, $\Pi_D \mathfrak{A}_i \models \varphi$.

(ii) For each finite subset F of Σ , let $I_F = \{i \in I \mid \mathfrak{A}_i \models F\}$; I_F is non-empty by hypothesis. Notice that $S = \{I_F \mid F \text{ is a finite subset of } \Sigma\}$ has FIP since $I_{F_1} \cap \dots \cap I_{F_n} \supseteq I_G$ where $G = \bigcup_{j=1}^n F_j$. Thus by Corollary 1.2, S is contained in an ultrafilter, D , over I . Since $I_{\{\varphi\}} \in D$, it follows from Corollary 3.2 that $\Pi_D \mathfrak{A}_i \models \varphi$ for every $\varphi \in \Sigma$. $\square$

As a corollary of the theorem we may obtain an algebraic proof of the Compactness Theorem discussed in the previous chapters.

5.2. COROLLARY. *If Σ is a set of sentences of L such that every finite subset of Σ has a model, then Σ has a model.*

PROOF. Let I be the set of all finite subsets of Σ and for each $i \in I$, let $\mathfrak{A}_i$ be a model of i . It is clear that the hypothesis of 5.1(ii) is satisfied, and

therefore there is an ultrafilter D over I such that $\Pi_D \mathfrak{A}_i$ is a model of Σ $\square$

Most, if not all, of the algebraic applications of ultraproducts which are given in this and the next two sections can be proved without use of ultraproducts by using instead Corollary 5.2, the Compactness Theorem. Many of them were first proved in this way. However, it is the goal of this paper to show how ultraproducts may be used to give more “algebraic” proofs. Thus our proofs are more-or-less direct applications of Theorem 5.1 or Theorem 3.1 and even the appeal to these general theorems can be replaced in specific applications by a direct verification from the definition of ultraproduct of the desired properties (cf. the remark at the end of the proof of 3.4).

5.3. THEOREM. *Let P be a infinite set of primes and for each $p \in P$ let F_p be a field of characteristic p . If D is a non-principal ultrafilter over P , then $\Pi_D F_p$ is a field of characteristic zero.*

PROOF. Let $\Sigma = \{\varphi_n \mid n \geq 1\}$ where φ_n is the sentence “ $n \cdot 1 \neq 0$ ”. For each n , $\{p \in P \mid F_p \models \varphi_n\}$ is cofinite since it is the set of primes in P not dividing n . Hence by 5.1 (i), $\Pi_D F_p$ is a model of Σ i.e. $\Pi_D F_p$ has characteristic zero. $\square$

A class is *finitely axiomatizable* (in L) if it is of the form $\mathcal{M}(\Sigma)$ where Σ is a finite set of sentences of L ; notice that in this case we may assume — by forming the conjunction of the sentences in Σ — that Σ consists of a single sentence. If $\mathcal{A} = \mathcal{M}(\{\theta\})$ is a finitely axiomatizable subclass of $\mathcal{M}(L)$ then the complement of $\mathcal{A}$ in $\mathcal{M}(L)$ is finitely axiomatizable — it is $\mathcal{M}(\{\neg \theta\})$ — and hence, by 3.3, closed under ultraproducts. Since by 5.3, the class of fields of non-zero characteristic is not closed under ultraproducts we obtain the following.

5.4. COROLLARY. *The class of fields of characteristic zero is axiomatizable but not finitely axiomatizable.*

Similarly we can prove the following. (For a proof and other examples of non-finite axiomatizability, see Chapter 5, §3, of BELL and SLOMSON [1969].)

5.5. THEOREM (Tarski). *The class of algebraically closed fields is axiomatizable but not finitely axiomatizable.*

5.6. THEOREM. *If φ is a sentence of the language of fields which is true in every field (resp. every algebraically closed field) of characteristic zero, then there is a finite set of primes P_φ such that φ is true in every field (resp. every algebraically closed field) of characteristic p if $p \notin P_\varphi$.*

PROOF. Suppose not. Then there is an infinite set of primes P such that for each $p \in P$ there is a field (resp. algebraically closed field) F_p which is a model of $\neg \varphi$. By 5.3 and 3.2, if D is a non-principal ultrafilter over P , $\Pi_D F_p$ is a field (resp. algebraically closed field) of characteristic zero which is a model of $\neg \varphi$, a contradiction. $\square$

We close this section with a definition which plays an important role in a very deep result of Ax [1968] that the theory of finite fields is decidable. Let Σ be the set of all sentences of the language of fields which are true in every finite field. An infinite model of Σ is called a *pseudofinite* field. (Ax [1968] gives a purely algebraic description of these fields.) The following immediate corollary of 5.1(i) shows how pseudofinite fields may be constructed as ultraproducts.

5.7. COROLLARY. *Let $\langle F_n : n \in \omega \rangle$ be a family of finite fields such that for each m , $\{n \in \omega \mid \text{cardinality of } F_n \leq m\}$ is finite. Let D be a non-principal ultrafilter over ω . Then $\Pi_D F_n$ is pseudofinite.* $\square$

6. Embedding theorems

The following theorem is an abstraction of a method frequently employed in proofs involving ultraproducts (cf. KEGEL and WEHRFRITZ [1973]), p. 66; also GRATZER [1968], Theorem 7, p. 261).

A set $\{\mathfrak{B}_i \mid i \in I\}$ of substructures of $\mathfrak{B}$ is called a *local system* for $\mathfrak{B}$ if: (1) $B = \bigcup \{B_i \mid i \in I\}$; and (2) for every $i, j \in I$ there exists $k \in I$ such that $B_i \cup B_j \subset B_k$. For example, the set of all finitely-generated substructures of $\mathfrak{B}$ is a local system for $\mathfrak{B}$.

6.1. THEOREM. *Let $\{\mathfrak{B}_i \mid i \in I\}$ be a local system for a model $\mathfrak{B} \in \mathcal{M}(\mathcal{L})$. Suppose $\langle \mathfrak{A}_i : i \in I \rangle$ is an indexed family of members of $\mathcal{M}(\mathcal{L})$ such that for each $i \in I$, there is an embedding (resp. homomorphism) of $\mathfrak{B}_i$ into $\mathfrak{A}_i$. Then there is an ultrafilter D on I and an embedding (resp. homomorphism) of $\mathfrak{B}$ into $\Pi_D \mathfrak{A}_i$.*

PROOF. Choose an embedding (resp. homomorphism) $\zeta_i : \mathfrak{B}_i \rightarrow \mathfrak{A}_i$ for each $i \in I$. For each $j \in I$, let $S_j = \{i \in I \mid B_j \subset B_i\}$. Then $S = \{S_j \mid j \in I\}$ has the FIP since $S_{j_1} \cap \cdots \cap S_{j_n} \supset S_k$ where k is such that $B_{j_1} \cup \cdots \cup B_{j_n} \subset B_k$. Hence by Corollary 1.2, S is contained in an ultrafilter D over I . For each $j \in I$, there is an embedding (resp. homomorphism) $\eta_j : \mathfrak{B}_j \rightarrow \Pi_D \mathfrak{A}_i$ given by: $g_j(b) = b_D$ where $\tilde{b}(i) = \zeta_i(b)$ if $i \in S_j$ and $\tilde{b}(i)$ is arbitrary otherwise. Now by definition of a local system, $\mathfrak{B}$ is the direct limit of the direct system consisting of the $\mathfrak{B}_i$, $i \in I$, and inclusion maps between them. The functions $\{\eta_j \mid j \in I\}$ form a compatible family of maps with respect to this direct system and hence they induce a function $\eta : \mathfrak{B} \rightarrow \Pi_D \mathfrak{A}_i$ which is easily seen to be an embedding (resp. homomorphism). $\square$

6.2. COROLLARY. *If $\mathcal{A} \subset \mathcal{M}(L)$ is closed under ultraproducts and if every finitely-generated substructure of $\mathfrak{B} \in \mathcal{M}(L)$ is embeddable in a member of $\mathcal{A}$, then $\mathfrak{B}$ is embeddable in a member of $\mathcal{A}$. $\square$*

A group G is called a *linear group of degree n* if it is isomorphic to a subgroup of $GL(n, F)$ for some field F . The following is an immediate consequence of Corollary 6.2 and Theorem 4.5.

6.3. THEOREM (MAL'CEV [1940]). *Let G be a group such that every finitely generated subgroup of G is a linear group of degree n . Then G is a linear group of degree n . $\square$*

For the sake of simplicity of exposition and proof we shall assume for the remainder of this section that our language L has a finite vocabulary, i.e. only a finite number of relation, function and constant symbols. If $\mathfrak{A}$ is a model for L an *equation over $\mathfrak{A}$* is an expression of the form $\gamma_0 = f(\gamma_1 \cdots \gamma_n)$ or $R(\gamma_1 \cdots \gamma_n)$ where f (resp. R) is an n -ary function (resp. relation) symbol and each γ_i is a variable or constant symbol of L or an element of A (or, more precisely, a new symbol c_a representing an element a of A). An *inequation over $\mathfrak{A}$* is the negation of an equation over $\mathfrak{A}$. If $\mathfrak{A} \subset \mathfrak{B}$ we say $\mathfrak{A}$ is *algebraically closed* (resp. *existentially closed*) in $\mathfrak{B}$ if any finite system of equations (resp. equations and inequations) over $\mathfrak{A}$ which has a solution in $\mathfrak{B}$ has a solution in $\mathfrak{A}$. We say $\mathfrak{A} \in \mathcal{A}$ is *algebraically closed* (resp. *existentially closed*) in $\mathcal{A}$ if $\mathfrak{A}$ is algebraically closed (resp. existentially closed) in every extension which is a member of $\mathcal{A}$. (A synonym for *existentially closed* is *existentially complete*. For more on these notions see Chapter A.4.)

6.4. THEOREM. Suppose $\mathfrak{A} \subset \mathfrak{B}$. Then $\mathfrak{A}$ is algebraically closed (resp. existentially closed) in $\mathfrak{B}$ if and only if there is an ultrafilter D and a commutative diagram

$$\begin{array}{ccc} & \Pi_D \mathfrak{A} & \\ d(\mathfrak{A}) \uparrow & \eta \searrow & \\ & \mathfrak{A} \subset \mathfrak{B} & \end{array}$$

such that η is a homomorphism (resp. embedding).

PROOF. For sufficiency, notice that η carries a solution of a finite system S of equations (resp. equations and inequations) with parameters from A into a solution of $d(S)$ —i.e. S with parameter a replaced by $d(a)$ —in $\Pi_D \mathfrak{A}$. If $b_D^{(1)}, \dots, b_D^{(m)}$ is a solution of $d(S)$ in $\Pi_D \mathfrak{A}$, then by Theorem 3.1 there is a (non-empty) set X in D such that for each $i \in X$, $b^{(1)}(i), \dots, b^{(m)}(i)$ is a solution of S in $\mathfrak{A}$. (Alternately, one may use the fact (4.7) that d is an elementary embedding: a fortiori $d(\mathfrak{A})$ is existentially closed in $\Pi_D \mathfrak{A}$.)

For necessity, we first note that without loss of generality we may assume that L has no function symbols (by replacing functions by their graphs). Let I be the set of all pairs (F_1, F_2) where F_1 is a finite subset of A including the interpretations of all constant symbols of L , and F_2 is a finite subset of $B - A$. Given $i = (F_1, F_2) \in I$, where, say, $F_2 = \{b_1 \cdots b_n\}$, let S be the set of all equations (resp. equations and inequations) in $x_1 \cdots x_n$ with constants from F_1 which are satisfied in $\mathfrak{B}$ when we let $x_j = b_j$ for $j = 1, \dots, n$. Since S is finite, S has a solution $x_1 = a_1, \dots, x_n = a_n$ in $\mathfrak{A}$. If $\mathfrak{B}_i$ denotes the substructure of $\mathfrak{B}$ with universe $F_1 \cup F_2$ (here we use the fact that L has no function symbols) then there is a homomorphism (resp. embedding) $\zeta_i : \mathfrak{B}_i \rightarrow \mathfrak{A}$ such that ζ_i is the identity on F_1 and $\zeta_i(b_j) = a_j$ for $j = 1, \dots, n$. Applying Theorem 6.1 to the local system $\{\mathfrak{B}_i \mid i \in I\}$, we obtain the desired homomorphism (resp. embedding) $\eta : \mathfrak{B} \rightarrow \Pi_D \mathfrak{A}$. $\square$

In similar fashion one can give necessary and sufficient conditions for $\mathfrak{A}$ to be an elementary substructure of $\mathfrak{B}$ (see BELL and SLOMSON [1969], Chapter 8, §1). The following nice application of 6.4 is due to SABBAGH [unpublished] and BACSICH [1972]. (Special cases were previously known; for example the case of group is due to NEUMANN [1952].) A model $\mathfrak{A} \in \mathcal{A}$ is called *simple in $\mathcal{A}$* if every non-constant morphism in $\mathcal{A}$ with domain $\mathfrak{A}$ is one-one.

6.5. THEOREM. *Suppose $\mathcal{A}$ is closed under ultraproducts and suppose every member of $\mathcal{A}$ can be embedded in a simple member of $\mathcal{A}$. If $\mathfrak{A}$ is algebraically closed in $\mathcal{A}$ and non-trivial (i.e. has cardinality ≥ 2), then $\mathfrak{A}$ is existentially closed in $\mathcal{A}$ and $\mathfrak{A}$ is simple in $\mathcal{A}$.*

PROOF. To prove the first part we must show that if $\mathfrak{A}$ is a submodel of $\mathfrak{B} \in \mathcal{A}$, then $\mathfrak{A}$ is existentially closed in $\mathfrak{B}$. By hypothesis, we may assume that $\mathfrak{B}$ is simple. By 6.4 there is a commutative diagram

$$\begin{array}{ccc} & \Pi_D \mathfrak{A} & \\ d(\mathfrak{A}) \uparrow & \nearrow \eta & \\ \mathfrak{A} \subset \mathfrak{B} & & \end{array}$$

where η is a homomorphism. Now η is not constant since $\mathfrak{A}$ is non-trivial. Hence η is one-one and so by 6.4 $\mathfrak{A}$ is existentially closed in $\mathfrak{B}$.

To see that $\mathfrak{A}$ is simple, consider a non-constant homomorphism $f: \mathfrak{A} \rightarrow \mathfrak{C}$. Now $\mathfrak{A}$ can be embedded in a simple model $\mathfrak{S}$ and by 6.4 and 4.7, we have a commutative diagram

$$\begin{array}{ccccc} \mathfrak{S} & \xrightarrow{\eta} & \Pi_D \mathfrak{A} & \xrightarrow{\Pi_D f} & \Pi_D \mathfrak{C} \\ & \searrow & \nearrow d(\mathfrak{A}) & & \nearrow d(\mathfrak{C}) \\ & \mathfrak{A} & \xrightarrow{\quad} & \mathfrak{C} & \end{array}$$

where η is a homomorphism. Since $d(\mathfrak{C})$ is one-one, $\Pi_D f \circ \eta$ is non-constant and therefore (since $\mathfrak{C}$ is simple) one-one. Since the diagram commutes, we conclude that f is one-one. $\square$

We conclude this section with a result about embeddings of rings due to A. Robinson and M. Rabin (see ROBINSON [1962]). We could derive the result from Theorem 6.1, but it is simpler to give a direct proof. A ring R (possibly without an identity) is called a *prime ring* if for all non-zero α and β in R , $\alpha R \beta$ is non-zero.

6.7. THEOREM. *Let $\mathcal{A}$ be a class of rings closed under ultraproducts. If R is a prime ring which is embeddable in a direct product of rings in $\mathcal{A}$, then R is embeddable in a member of $\mathcal{A}$.*

PROOF. Suppose $R \subset \Pi_I A_i$, where $A_i \in \mathcal{A}$ for all $i \in I$. For each non-zero

α in R let $S_\alpha = \{i \in I \mid \alpha(i) \neq 0\}$. Since R is a prime ring, $S = \{S_\alpha \mid \alpha \neq 0, \alpha \in R\}$ has FIP (because $S_\alpha \cap S_\beta \supset S_{\alpha\gamma\beta}$ for some $\gamma \in R$). Thus by Corollary 1.2, S is contained in an ultrafilter D over I . Let $A = \prod_D A_i$. By hypothesis, $A \in \mathcal{A}$. Define a map $\eta : R \rightarrow A$ by $\eta(\alpha) = \alpha_D$; then η is an embedding since for each non-zero α in R , $S_\alpha \in D$. $\square$

The following corollary is due to ROBINSON [1962] for the case of division rings, and AMITSUR [1967] for the case of primitive rings. See AMITSUR [1967], HERSTEIN [1968], Chapter 7 or HIRSCHELMANN [1972] for generalizations and an important application to Posner's Theorem.

6.8. COROLLARY. *If R is a prime ring which is a subring of a direct product of division rings (resp. primitive rings), then R is a subring of a division ring (resp. primitive ring).*

PROOF. The class of division rings is elementary, hence closed under ultraproducts. The class of primitive rings is pseudo-elementary, hence closed under ultraproducts (see Theorem 4.6). $\square$

Some more applications of Theorem 6.7 to the study of polynomial identities and rational identities of division rings can be found in AMITSUR [1965 and 1966].

7. Bounds in polynomial ideals

Throughout this section we shall be considering polynomial rings $F[X_1 \cdots X_n]$ over a field F , where n is an arbitrary but fixed positive integer. A polynomial in $F[X_1 \cdots X_n]$ will be written as $f = \sum_M c_M X^M$ where M ranges over all n -tuples $(m_1 \cdots m_n)$ of natural numbers and X^M is an abbreviation for $X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n}$. The *degree* of M , denoted $\delta(M)$, is $\sum_{i=1}^n m_i$; and the degree of f is $\max\{\delta(M) \mid c_M \neq 0\}$.

Let $\langle F_i : i \in I \rangle$ be an indexed family of fields and let D be an ultrafilter over I . Let $\bar{F}$ denote the field $\prod_D F_i$ and for $c \in \prod_I F_i$ let $\bar{c}$ denote c_D . Let R denote the ring $\prod_D (F_i[X_1 \cdots X_n])$. Now R is not a polynomial ring over $\bar{F}$ —it is not even Noetherian—but there is a canonical mapping

$$\mu : \bar{F}[X_1 \cdots X_n] \rightarrow R$$

defined as follows. If $f = \sum_M \bar{c}_M X^M \in \bar{F}[X_1 \cdots X_n]$ and $\deg f = d$, then $\mu(f) = f_D$ where $f(i) = \sum_{\delta(M) \leq d} c_M(i) X^M$.

An indexed family $f = \langle f_i : i \in I \rangle$ of polynomials $f_i \in F_i [X_1 \cdots X_n]$ is called *bounded* if there exists m such that $\deg f_i \leq m$ for all $i \in I$. We leave to the reader the task of checking the following.

7.1. THEOREM. *The function μ is a well-defined embedding of rings whose range is the subring of elements of R represented by bounded families. Moreover, for any $f \in \bar{F}[X_1 \cdots X_n]$ and any $\bar{a}_1, \dots, \bar{a}_n \in \bar{F}$, we have $f(\bar{a}_1 \cdots \bar{a}_n) = \bar{v}$, where $v(i) = f(i)(a_1(i) \cdots a_n(i))$.*

If $f = \langle f_i : i \in I \rangle$ is a bounded family, let $\bar{f}$ denote the unique element of $\bar{F}[X_1 \cdots X_n]$ such that $\mu(\bar{f}) = f_D$. As a consequence of 7.1 and the fundamental theorem we obtain the following.

7.2. COROLLARY. *Let $f = \langle f_i : i \in I \rangle$, $g^{(l)} = \langle g_i^{(l)} : i \in I \rangle$, $h^{(l)} = \langle h_i^{(l)} : i \in I \rangle$ be bounded families of polynomials, for $l = 1, \dots, r$. Then*

$$\bar{f} = \sum_{l=1}^r \bar{g}^{(l)} \bar{h}^{(l)} \quad \text{iff} \quad \left\{ i \in I \mid f_i = \sum_{l=1}^r g_i^{(l)} h_i^{(l)} \right\} \in D.$$

Moreover, for any $\bar{a}_1, \dots, \bar{a}_n$ in $\bar{F}$, $\bar{f}(\bar{a}_1 \cdots \bar{a}_n) = \bar{0}$ if and only if $\{i \in I \mid f_i(a_1(i) \cdots a_n(i)) = 0\} \in D$. $\square$

Let us consider some applications.

7.3. THEOREM (ROBINSON [1955a]). *Given positive integers n and d there exists a positive integer m such that for any algebraically closed field F and any polynomials $f, g^{(1)}, \dots, g^{(r)}$ in $F[X_1 \cdots X_n]$ of degree $\leq d$, if every common zero of $g^{(1)}, \dots, g^{(r)}$ in F is a zero of f , then f^m belongs to $\langle g^{(1)}, \dots, g^{(r)} \rangle$, the ideal generated by $g^{(1)}, \dots, g^{(r)}$.*

PROOF. Note that the content of the theorem is that m can be chosen to depend only on n and d . Hilbert's Nullstellensatz, which we use in the proof, asserts that given $f, g^{(1)}, \dots, g^{(r)}$ satisfying the hypotheses, there is some m —a priori depending on $f, g^{(1)}, \dots, g^{(r)}$ —such that $f^m \in \langle g^{(1)}, \dots, g^{(r)} \rangle$. If the theorem is false, then for each $i \in I = \omega$ there exists an algebraically closed field F_i and polynomials $f_i, g_i^{(1)}, \dots, g_i^{(r)} \in F_i[X_1 \cdots X_n]$ of degree $\leq d$ such that $f_i \notin \langle g_i^{(1)}, \dots, g_i^{(r)} \rangle$ but every zero of $g_i^{(1)} \cdots g_i^{(r)}$ in F_i is a zero of f_i . (Note that we can assume that r does not depend on i since every ideal generated by polynomials of degree $\leq d$ has a basis of cardinality $\leq$ the dimension (over the field of coefficients) of the vector space of polynomials of degree $\leq d$.) Let D be a non-principal ultrafilter

over I . Since $\langle f_i : i \in I \rangle$ and $\langle g_i^{(l)} : i \in I \rangle$, $l = 1, \dots, r$ are bounded families we may consider $\bar{f}, \bar{g}^{(1)}, \dots, \bar{g}^{(r)} \in \bar{F}[X_1 \cdots X_n]$. Every zero of $\bar{g}^{(1)}, \dots, \bar{g}^{(r)}$ in $\bar{F}$ is a zero of $\bar{f}$ by Corollary 7.2 since this is true for all $i \in I$. Hence by the Nullstellensatz, $\bar{f}^k \in \langle \bar{g}^{(1)}, \dots, \bar{g}^{(r)} \rangle$ for some $k \in \omega$. Then by 7.2 we have $\{i \in I \mid f_i^k \in \langle g_i^{(1)}, \dots, g_i^{(r)} \rangle\} \in D$. But this contradicts the choice of $f_i, g_i^{(1)}, \dots, g_i^{(r)}$ and the fact that every element of D is infinite. $\square$

The following result, giving bounds for Hilbert's basis theorem, is proved in a similar fashion. (See SEIDENBERG [1971] for a purely algebraic proof.)

7.4. THEOREM. *Given positive integers n and d there exists m such that for any field F , any strictly ascending chain of ideals in $F[X_1 \cdots X_n]$ which are generated by polynomials of degree $\leq d$ is of length $\leq m$.*

One can also employ these methods in order to obtain bounds for the number of squares required to represent a positive definite rational functional over an ordered field as a sum of squares (see, for example, ROBINSON [1973b]).

The following result about bounds requires a different mode of proof (see ROBINSON [1973a] for a discussion of the difference). It was first proved by KÖNIG [1903] and HERMANN [1926] using complex computational methods. The following proof is due to ROBINSON [1973a].

7.5. THEOREM. *Given positive integers n and d there exists m such that for any field F and any polynomials $f, g^{(1)}, \dots, g^{(r)}$ in $F[X_1 \cdots X_n]$ of degree $\leq d$, if $f \in \langle g^{(1)}, \dots, g^{(r)} \rangle$, then there exist polynomials $h^{(1)}, \dots, h^{(r)}$ in $F[X_1 \cdots X_n]$ of degree $\leq m$ such that $f = \sum_{i=1}^r h^{(i)} g^{(i)}$.*

PROOF. By standard considerations of linear algebra it suffices to prove the theorem for algebraically closed fields. Suppose the theorem is false. Then for every $i \in I = \omega$ there exists an algebraically closed field F_i and polynomials $f_i, g_i^{(1)}, \dots, g_i^{(r)} \in F_i[X_1 \cdots X_n]$ of degree $\leq d$ such that $f_i \in \langle g_i^{(1)}, \dots, g_i^{(r)} \rangle$, but there are no polynomials $h_i^{(1)}, \dots, h_i^{(r)}$ of degree $\leq i$ such that $f_i = \sum_{i=1}^r h_i^{(i)} g_i^{(i)}$. Let D be a non-principal ultrafilter over I and consider $\bar{f}, \bar{g}^{(1)}, \dots, \bar{g}^{(r)} \in \bar{F}[X_1 \cdots X_n]$. Let G denote $\langle \bar{g}^{(1)}, \dots, \bar{g}^{(r)} \rangle$, the ideal generated by $\bar{g}^{(1)}, \dots, \bar{g}^{(r)}$ in $\bar{F}[X_1 \cdots X_n]$. If we can prove that $\bar{f} \in G$ then we will be done since then there will exist $\bar{h}^{(1)}, \dots, \bar{h}^{(r)}$ in $\bar{F}[X_1 \cdots X_n]$ such that $\bar{f} = \sum_{i=1}^r \bar{h}^{(i)} \bar{g}^{(i)}$, and this, by 7.2, will contradict the choice of the $f_i, g_i^{(1)}, \dots, g_i^{(r)}$.

Since the case $G = \bar{F}[X_1 \cdots X_n]$ is trivial, we may assume that $G =$

$Q_1 \cap \cdots \cap Q_k$ where the Q_j 's are proper primary ideals (cf. ZARISKI and SAMUEL [1958], Chapter IV, §4). So it suffices to prove that $\bar{f} \in Q_j$ for $j = 1, \dots, k$. Consider a fixed $Q_j = Q$. By a change of coordinates we may assume that $Q \subset \langle X_1, \dots, X_n \rangle$. (If $(a_1, \dots, a_n)$ is a zero of Q in F , let $Y_\nu = X_\nu - a_\nu$ for $\nu = 1, \dots, n$.) Let P denote $\langle X_1, \dots, X_n \rangle$. By the Krull Intersection Theorem (ZARISKI and SAMUEL [1958], Chapter IV, Theorem 12'), it suffices to prove that $f \in Q + P^m$ for every $m \geq 0$.

Now since $f_i \in \langle g_i^{(1)}, \dots, g_i^{(r)} \rangle$, there exist polynomials $p_i^{(1)} \cdots p_i^{(r)}$ such that $f_i = \sum_{i=1}^r p_i^{(1)} g_i^{(1)}$. Let $p_D^{(i)}$ be the class of $\langle p_i^{(i)} : i \in I \rangle$ in R . Then $f_D = \sum_{i=1}^r p_D^{(i)} g_D^{(i)}$, i.e. $\mu(\bar{f}) = \sum_{i=1}^r p_D^{(i)} \mu(\bar{g}^{(i)})$. Fix $m > 0$. Let $q_D^{(i)}$ be the class of $\langle q_i^{(i)} : i \in I \rangle$ where $q_i^{(i)} = \sum_{\delta(M) \leq m} c_M(i) X^M$ if $p_i^{(i)} = \sum_M c_M(i) X^M$. Notice that $q_D^{(i)}$ belongs to the range of μ ; say $q_D^{(i)} = \mu(\bar{q}^{(i)})$. Then

$$\mu(\bar{f}) - \sum_{i=1}^r \mu(\bar{q}^{(i)}) \mu(\bar{g}^{(i)}) = \sum_{i=1}^r (p_D^{(i)} - q_D^{(i)}) g_D^{(i)}.$$

The left-hand side clearly belongs to the range of μ ; thus the right-hand side shows that it belongs to $\mu(P^m)$. We conclude that $\bar{f} \in Q + P^m$. $\square$

The following result is due to HERMANN [1926] (see also SEIDENBERG [1974]). It would be of interest to have an ultraproduct proof of this result in the spirit of the above, avoiding the computational methods of Hermann. None is known at present.

7.6. THEOREM. *Given positive integers n and d there exists m such that for any ideal J of $F[X_1 \cdots X_n]$ which has a basis consisting of polynomials of degree $\leq d$, if J is not prime, then there exist polynomials f, g of degree $\leq m$ such that $fg \in J$ but $f \notin J$ and $g \notin J$.*

For an application of the methods of this section and Section 5 to the problem of resolutions of singularities in algebraic geometry, see EKLOF [1969].

SATURATION

8. Ultraproducts which are ω_1 -saturated

In Sections 5–7 we used ultraproducts to construct models which satisfied given sets Σ of first-order properties. Now we want to study a property of ultraproducts (with respect to certain ultrafilters) called ω_1 -saturation

which is not first-order but which is model-theoretic in character and is very useful in studying first-order properties of models.

Recall from Chapter A.2 that if $\mathfrak{A}$ is a model for L and X is a subset of A , then L_X denotes the language obtained by adding a constant symbol c_a for each $a \in X$; and $\mathfrak{A}_X = (\mathfrak{A}, a)_{a \in X}$ is the model for L_X obtained by interpreting the new constant c_a by the element a . Let $\Gamma(v)$ be a set of formulas $\gamma(v)$ of L_X which have v as the only free variable; $\Gamma(v)$ is called a *type in $\mathfrak{A}_X$* if for every finite subset $\{\gamma_0(v), \dots, \gamma_m(v)\}$ of $\Gamma(v)$ there exists $a \in A$ such that $\mathfrak{A}_X \models \gamma_i[a]$ for $i = 0, \dots, m$. We say Γ is *realized* in $\mathfrak{A}_X$ if there exists $a \in A$ such that $\mathfrak{A}_X \models \gamma[a]$ for all $\gamma(v)$ in $\Gamma(v)$. A model $\mathfrak{A}$ for L is called ω_1 -saturated if for every countable subset X of A , every type in $\mathfrak{A}_X$ is realized in $\mathfrak{A}_X$. In order to clarify the definition let us begin with two important examples. A linearly ordered set $\mathfrak{A}$ is called an η_α -set (HAUSDORFF [1914]) if whenever B_1 and B_2 are subsets of A of cardinality $< \omega_\alpha$ such that $B_1 < B_2$ (i.e. for all $b_1 \in B_1, b_2 \in B_2$, we have $b_1 < b_2$), then there exists $a \in A$ such that $B_1 < a < B_2$ (i.e. for all $b_1 \in B_1, b_2 \in B_2$ we have $b_1 < a < b_2$). Obviously an η_0 -set is just a densely ordered set without first or last element.

8.1. LEMMA. *If $\mathfrak{A}$ is an η_0 -set which is ω_1 -saturated, then $\mathfrak{A}$ is an η_1 -set.*

PROOF. Suppose B_1 and B_2 are countable subsets of A such that $B_1 < B_2$. Let $X = B_1 \cup B_2$ and $\Gamma(v)$ be the set of all formulas of L_X of the form

$$c_{b_1} < v < c_{b_2}$$

where $b_1 \in B_1$ and $b_2 \in B_2$. Since $\mathfrak{A}$ is an η_0 -set, $\Gamma(v)$ is a type in $\mathfrak{A}_X$. Therefore $\Gamma(v)$ is realized in $\mathfrak{A}_X$ by some $a \in A$. It is then clear that $B_1 < a < B_2$. $\square$

(The converse of Lemma 8.1 is true but we are not concerned with it here. In Section 10, we deal with the more general definition of ω_α -saturated models; 8.1 has a natural analog in that setting.)

8.2. LEMMA. *If $\mathfrak{A}$ is an infinite model which is ω_1 -saturated, then $\mathfrak{A}$ is uncountable.*

PROOF. Suppose to the contrary that A is countable. Let $\Gamma(v)$ be the set of all formulas of L_A of the form

$$v \neq c_a$$

where $a \in A$. Since A is infinite, $\Gamma(v)$ is a type in $\mathfrak{A}_A$ and hence is realized in $\mathfrak{A}_A$, which is impossible. $\square$

We are going to prove that ultraproducts over the right kind of ultrafilter are ω_1 -saturated; for this we need a new class of ultrafilters. An ultrafilter D over I is called ω_1 -incomplete if there exist pairwise disjoint subsets Y_n of I such that $\bigcup_{n \in \omega} Y_n = I$ but for all $n \in \omega$, $Y_n \notin D$. An ω_1 -incomplete ultrafilter is clearly non-principal since for a principal ultrafilter there exists $a \in I$ such that $Y \in D$ if and only if $a \in Y$. The converse holds if I is countable.

8.3. LEMMA. *Every non-principal ultrafilter on a countable set I is ω_1 -incomplete.*

PROOF. Say $I = \{a_n : n \in \omega\}$. Let $Y_n = \{a_n\}$. Then $Y_n \notin D$ since D is non-principal, but $\bigcup_n Y_n = I$. $\square$

It is consistent with the usual axioms of set theory (ZFC) to assume that 8.3 holds for sets I of any infinite cardinality. However it is an open problem of set theory whether 8.3 can be proved (from ZFC) to hold for all infinite sets I . It is known that if 8.3 fails for I , then I is extraordinarily large. The cardinality of the smallest such I is a measurable cardinal, as discussed in the anonymous appendix to Chapter B.3.

8.4. LEMMA. *For any infinite set I there is an ω_1 -incomplete ultrafilter over I .*

PROOF. Since I is infinite we can write $I = \bigcup_{n \in \omega} Y_n$ where the Y_n 's are pairwise disjoint and infinite. Let $S = \{I - Y_n : n \in \omega\}$. Then S has FIP so by Corollary 1.2, S is contained in an ultrafilter D which is ω_1 -incomplete by construction. $\square$

8.5. THEOREM. *Let L be a countable language and let D be an ω_1 -incomplete ultrafilter over I . For any family $\langle \mathfrak{A}_i : i \in I \rangle$ of models for L , the ultraproduct $\Pi_D \mathfrak{A}_i$ is ω_1 -saturated.*

PROOF. Let X be a countable subset of $\Pi_D A_i$ and $\Gamma(v)$ a type in $(\Pi_D \mathfrak{A}_i)_X$. Say $\Gamma(v) = \{\gamma_n(v) : n \in \omega\}$. (Notice that Γ is countable since L is countable.) Let Y_n , $n \in \omega$, be subsets of I such that $Y_n \notin D$ but $\bigcup_{n \in \omega} Y_n = I$. Since $\Gamma(v)$ is a type in $\Pi_D \mathfrak{A}_i$ there exists for every $m \in \omega$ an element $f_D^{(m)}$ of $\Pi_D A_i$ such that $\Pi_D \mathfrak{A}_i \models \gamma_n[f_D^{(m)}]$ for $n = 1, \dots, m$. Now define $g \in \Pi_I A_i$

by $g(i) = f^{(m)}(i)$ if $i \in Y_m$. We claim that $\Pi_D \mathfrak{A}_i \models \gamma_m[g_D]$ for all $m \in \omega$. By Theorem 3.1 it suffices to prove that $\{i \in I \mid \mathfrak{A}_i \models \gamma_m[g(i)]\} = Z_m$ is in D . But Z_m contains $I - \bigcup_{n=0}^{m-1} Y_n = \bigcap_{n=0}^{m-1} (I - Y_n)$ and hence is in D since $Y_n \notin D$ for all n . $\square$

A first-order theory T is said to be *model-complete* if whenever $\mathfrak{A}$ and $\mathfrak{B}$ are models of T such that $\mathfrak{A}$ is a submodel of $\mathfrak{B}$, then $\mathfrak{A}$ is an elementary submodel of $\mathfrak{B}$. For more on model-completeness see Chapter A.4. Here we simply want to show how ultraproducts may be used to prove that a theory is model-complete.

8.6. THEOREM (Robinson). *The theory of real-closed fields is model-complete.*

PROOF. We shall assume the continuum hypothesis (CH). Suppose $R_1 \subset R_2$ are real-closed fields. Let $\varphi(v_1 \cdots v_n)$ be a formula of the language of fields and let $a_1, \dots, a_n \in R_1$ such that $R_1 \models \varphi[a_1 \cdots a_n]$. We wish to prove that $R_2 \models \varphi[a_1 \cdots a_n]$. We claim that we may assume that R_1 and R_2 are countable. By the Lowenheim–Skolem theorem (see Chapter A.2) there is a countable elementary submodel R'_1 of R_1 containing $a_1, \dots, a_n$, and there is a countable elementary submodel R'_2 of R_2 containing R'_1 . Thus we have countable real-closed fields $R'_1 \subset R'_2$, $R'_1 \models \varphi[a_1, \dots, a_n]$, and we wish to prove that $R'_2 \models \varphi[a_1, \dots, a_n]$. This proves the claim.

Let D be a non-principal ultrafilter on a countable set I . By Theorem 4.7 there are elementary embeddings $d(R_\nu): R_\nu \rightarrow \Pi_D R_\nu$, for $\nu = 1, 2$. By 8.3 and 8.5, $\Pi_D R_\nu$ is ω_1 -saturated and by 8.1 $\Pi_D R_\nu$ is an η_1 -set (with respect to the unique ordering on a real closed field) for $\nu = 1, 2$. By a result of ERDOS, GILLMAN and HENRIKSEN [1955] any two real closed fields of cardinality $\aleph_1$ which are η_1 -sets are isomorphic, in fact any isomorphism of countable subfields extends to an isomorphism of the real-closed fields. Now by Lemma 8.2, $\text{Card}(\Pi_D R_\nu) \geq \aleph_1$. But $\text{Card}(\Pi_D R_\nu) \leq \text{Card}(\Pi_I R_\nu) = 2^{\aleph_0} = \aleph_1$. Hence $\text{Card}(\Pi_D R_\nu) = \aleph_1$ for $\nu = 1, 2$. Therefore by the result cited above, if $e: R_1 \rightarrow R_2$ is the inclusion map, there is an isomorphism $\phi: \Pi_D R_1 \rightarrow \Pi_D R_2$ such that

$$\begin{array}{ccc} \Pi_D R_1 & \xrightarrow{\phi} & \Pi_D R_2 \\ \uparrow d(R_1) & & \uparrow u(R_2) \\ R_1 & \xrightarrow{e} & R_2 \end{array}$$

commutes. Hence

$$\begin{aligned}
R_1 \models \varphi [a_1 \cdots a_n] &\Leftrightarrow \Pi_D R_1 \models \varphi [d(R_1)(a_1) \cdots d(R_1)(a_n)] \\
&\Leftrightarrow \Pi_D R_2 \models \varphi [\phi(d(R_1)(a_1)) \cdots \phi(d(R_1)(a_n))] \\
&\Leftrightarrow \Pi_D R_2 \models \varphi [d(R_2)(a_1) \cdots d(R_2)(a_n)] \\
&\Leftrightarrow R_2 \models \varphi [a_1 \cdots a_n]. \quad \square
\end{aligned}$$

(Although we assumed CH in the proof it follows from general logical considerations—which we shall not give here—that the result actually holds without this assumption.)

Let us take the opportunity to mention that 8.6 has important algebraic consequences; in fact ROBINSON [1955b] (see also ROBINSON [1973b]) showed how the solution to Hilbert's seventeenth problem (solved originally by Artin) may be derived easily from Theorem 8.6. See 2.3 in Chapter A.4.

8.7. COROLLARY (Tarski). *The theory of real-closed fields is complete i.e. any two real-closed fields are elementarily equivalent.*

PROOF. This follows immediately from 8.6 and the fact that any real-closed field contains a copy of the real closure of the rationals (cf. Theorem 6 of 1.7 in Chapter A.4). $\square$

In similar fashion we may prove the following result, using the well-known theorem of Steinitz that any two algebraically closed fields of the same characteristic and the same uncountable cardinality are isomorphic.

8.8. THEOREM (Tarski–Robinson). *Let p be 0 or a prime. The theory of algebraically closed fields of characteristic p is complete and model-complete.*

The continuum hypothesis is not needed in the proof of 8.8 because of the following result (see BELL and SLOMSON [1969], p. 130, for a proof).

8.9. THEOREM. *If $\langle A_i : i \in I \rangle$ is a family of infinite sets and D is any ω_1 -incomplete ultrafilter over I , then the cardinality of $\Pi_D A_i$ is at least $2^{\aleph_0}$.*

We close with an interesting application of the methods of this and Section 5. The following is a special case of a theorem of Ax [1968].

8.10. THEOREM. *Let F be an algebraically closed field and let $\Psi : F^n \rightarrow F^m$*

be a polynomial map, i.e. $\Psi(x_1 \cdots x_n) = (\psi_1(x_1 \cdots x_n), \dots, \psi_m(x_1 \cdots x_n))$ where $\psi_1, \dots, \psi_m$ are elements of $F[X_1 \cdots X_n]$. If Ψ is injective, then Ψ is surjective.

PROOF. For a fixed n and m and fixed degrees for $\psi_1, \dots, \psi_m$ the theorem is expressible as a first-order sentence in the language of fields. Hence by Theorem 8.8 it suffices to prove the theorem for one algebraically closed field of each characteristic. For characteristic p , a prime, the theorem is easily seen to be true by a simple counting argument for $\tilde{F}_p$, the union of all the finite fields of characteristic p . The theorem is true for $\Pi_D \tilde{F}_p$, where D is a non-principal ultrafilter over P , the set of primes, by Corollary 3.2, and by Theorem 5.3, $\Pi_D \tilde{F}_p$ has characteristic zero. $\square$

9. Ultraproducts of valued fields

One of the most important applications of ultraproducts to algebra is the work of AX and KOCHEN [1965a, 1965b and 1966] and ERSHOV [1965] on Artin's Conjecture. The scope of this article dictates that we confine ourselves to giving an introduction to this work, sketching very briefly the role which ultraproducts play in the proof. We refer those whose appetite is whetted by this introduction to the original papers or to one of the many excellent expositions (e.g. CHANG and KEISLER [1973], KOCHEN [1975] and ROBINSON [1969]). See also the discussion in 2.4 of Chapter A.4.

Artin's Conjecture states that the following property holds for all n and d when $F = \mathbf{Q}_p$, the field of p -adic numbers.

($A_{n,d}$) Every homogeneous polynomial $f \in F[X_1 \cdots X_n]$ of degree d such that $n > d^2$ has a non-trivial zero in F .

The conjecture is inspired by the similarities between $\mathbf{Q}_p$ and $\mathbf{Z}_p((t))$, the field of formal power series over $\mathbf{Z}_p$, the field of order p . Lang proved that $\mathbf{Z}_p((t))$ satisfies the property $A_{n,d}$ for all n and d . Artin's Conjecture in fact has been shown to be false for some p by TERJANIAN [1966]. However, Ax-Kochen and Ershov proved the following.

9.1. THEOREM. *For any positive integers n and d there is a finite set of primes $P_0(n, d)$ such that for every prime $p \notin P_0(n, d)$, $A_{n,d}$ holds when $F = \mathbf{Q}_p$.*

At the heart of the proof of 9.1 is the following result which also gives a precise formulation of the intuitive analogy between $\mathbf{Q}_p$ and $\mathbf{Z}_p((t))$.

9.2. THEOREM. *For any non-principal ultrafilter D over P , the set of all primes, the ultraproducts $\Pi_D \mathbf{Q}_p$ and $\Pi_D \mathbf{Z}_p((t))$ are isomorphic fields.*

We leave to the reader the easy proof of 9.1 from 9.2. (Hint: use Corollary 3.2, Corollary 1.5, Lang's result and the fact that for fixed n and d , property $A_{n,d}$ is a first-order statement.)

As in the case of 8.6 and 8.8, Theorem 9.2 is proved by using algebraic properties possessed by the ultraproducts which arise from their being ω_1 -saturated. We shall not give the proof, which is considerably more sophisticated than those of 8.6 and 8.8, but we do want to indicate the key role played by ω_1 -saturation. In fact Ax and Kochen prove that $\Pi_D \mathbf{Q}_p$ and $\Pi_D \mathbf{Z}_p((t))$ are isomorphic as valued fields. Define a *valued field (with cross-section)* to be a model

$$F = \langle F, +, \cdot, 0, 1, A, \leq, | \cdot | \rangle$$

where $\langle F, +, \cdot, 0, 1 \rangle$ is a field; $\langle A, \cdot, 1, \leq \rangle$ is an ordered abelian group; $| \cdot | : F - \{0\} \rightarrow A$ is surjective and a valuation (i.e. $|xy| = |x| |y|$, $|x+y| \leq \max\{|x|, |y|\}$); and $|x| = x$ for all $x \in A$. F is said to be ω -pseudo-complete if for any sequence $\{a_n \mid n \in \omega\}$ of elements of F such that

$$(*) \quad |a_m - a_n| = |a_{n+1} - a_n|$$

whenever $n < m < \omega$, there exists $a \in F$ such that

$$|a - a_n| = |a_{n+1} - a_n|$$

for all $n \in \omega$. The crucial result is then the following.

9.3. THEOREM. *If F is an ω_1 -saturated valued field, then F is ω -pseudo-complete.*

PROOF. If $X = \{a_n \mid n \in \omega\}$ is a sequence in F satisfying $(*)$ —such a sequence is called ω -pseudo-Cauchy—let $\Gamma(v)$ be the set of all formulas

$$\gamma_n(v): |v - a_n| = |a_{n+1} - a_n|$$

for all $n \in \omega$. $\Gamma(v)$ is a subset of L_X , where L is the language of valued fields. Now $\Gamma(v)$ is a type in F_X since for any $m \in \omega$

$$F_X \models \gamma_n[a_{m+1}]$$

for $n = 0, \dots, m$. Therefore there exists $a \in F$ such that

$$F_x \models \gamma_n[a]$$

for all $n \in \omega$ (We say a is a *pseudo-limit* of X .) $\square$

10. Saturated models

In the short space left to us we define the κ -saturated and saturated models, which generalize the union of ω_1 -saturated models, and mention without proof some important facts about these models. For more details and proofs see CHANG and KEISLER [1973], CHANG [1973] or BELL and SLOMSON [1969].

Let κ be an infinite cardinal. A model $\mathfrak{A}$ for L is called κ -saturated if for every subset X of $\mathfrak{A}$ of cardinality $< \kappa$, every type in $\mathfrak{A}_X$ is realized in $\mathfrak{A}$. $\mathfrak{A}$ is called *saturated* if $\mathfrak{A}$ is κ -saturated where κ is the cardinality of $\mathfrak{A}$. As in Section 8 we can prove:

10.1. LEMMA. (i) *If $\mathfrak{A}$ is an infinite model which is κ -saturated, then $\mathfrak{A}$ has cardinality $\geq \kappa$.*

(ii) *If $\mathfrak{A}$ is an η_0 -set which is ω_α -saturated, then $\mathfrak{A}$ is an η_α -set.*

Models which are κ -saturated can be obtained as ultraproducts, though the proof is more difficult than that of Theorem 8.5. The following theorem was first proved by KEISLER [1964] using GCH and by KUNEN [1972] without GCH.

10.2. THEOREM. *Let L be a language of cardinality $\leq \kappa$ and let I be a set of power κ . Then there is an ultrafilter D on I such that for any family $\langle \mathfrak{A}_i : i \in I \rangle$ of models for L , the ultraproduct $\Pi_D \mathfrak{A}_i$ is κ^+ -saturated.*

(The ultrafilters with the property given by the above theorem are called κ^+ -good ultrafilters and were introduced by KEISLER [1964].) As a corollary we obtain the existence of saturated models. (The hypothesis of GCH at κ is essential.)

10.3. COROLLARY. *Let κ be a cardinal such that $2^\kappa = \kappa^+$. If $\mathfrak{A}$ is a model for L of cardinality $\leq \kappa$ (where L has cardinality $\leq \kappa$), then there is an elementary extension $\mathfrak{B}$ of $\mathfrak{A}$ of cardinality κ^+ which is saturated.*

PROOF. Let I and D be as in Theorem 10.2. Then $\mathfrak{B} = \Pi_D \mathfrak{A}$ is κ^+ -

saturated. By Theorem 4.7, $\mathfrak{B}$ is an elementary extension of $\mathfrak{A}$. Moreover $\kappa^+ \leq \text{Card}(B) \leq 2^\kappa$ by Lemma 10.1 and the definition of ultrapowers, so by hypothesis, $\text{Card}(B) = \kappa^+$ and hence $\mathfrak{B}$ is saturated. $\square$

A key property of saturated models is the following, due to Vaught (see MORLEY and VAUGHT [1962]). It explains the motivation behind the proofs of 8.6 and 8.8.

10.4. THEOREM. *Elementarily equivalent saturated models of the same cardinality are isomorphic.*

The following immediate consequence of 10.2 and 10.4 was also proved directly without GCH by SHELAH [1971].

10.5. COROLLARY (GCH). *Let $\mathfrak{A}$ and $\mathfrak{B}$ be models for the same language L . The following are equivalent:*

- (1) $\mathfrak{A}$ is elementarily equivalent to $\mathfrak{B}$.
- (2) There is an ultrafilter D on a set I such that $\Pi_D \mathfrak{A}$ is isomorphic to $\Pi_D \mathfrak{B}$.

Thus we see that elementary equivalence is an algebraic notion.

References

- AMITSUR, S.
 [1965] Generalized polynomial identities and pivotal monomials, *Trans. Am. Math. Soc.*, **114**, 210–226.
 [1966] Rational identities and applications to algebra and geometry, *J. Algebra*, **3**, 304–359.
 [1967] Prime rings having polynomial identities with arbitrary coefficients, *Proc. London Math.*, III, **17**, 470–486.
- AX, J.,
 [1968] The elementary theory of finite fields, *Ann. of Math.*, **88**, 239–271.
- AX, J., and S. KOCHEN
 [1965a] Diophantine problems over local fields I, *Am. J. Math.*, **87**, 605–630.
 [1965b] Diophantine problems over local fields II: A complete set of axioms for p -adic number theory, *Am. J. Math.*, **87**, 631–648.
 [1966] Diophantine problems over local fields III: Decidable fields, *Ann. of Math.*, **83**, 437–456.
- BACSICH, P.D.
 [1972] Cofinal simplicity and algebraic closedness. *Algebra Universalis*, **2**, 354–360.
- BELL, J.L. and A.B. SLOMSON
 [1969] *Models and Ultraproducts, an introduction* (North-Holland, Amsterdam).

CHANG, C.C.

- [1967] Ultraproducts and other methods of constructing models, in: *Sets, Models and Recursion Theory*, edited by J.N. Crossley (North-Holland, Amsterdam) pp. 85–121.

- [1973] What's so special about saturated models, in: *Studies in Model Theory*, edited by M. Morley, MAA Studies in Mathematics, Vol. 8 (Math. Assoc. Am., Buffalo, NY) pp. 59–65.

CHANG, C.C. and H.J. KEISLER

- [1973] *Model Theory* (North-Holland, Amsterdam).

EKLOF, P.

- [1969] Resolutions of singularities in prime characteristic for almost all primes, *Trans. Am. Math. Soc.*, **146**, 429–438.

ERDOS, P., L. GILLMAN and M. HENRIKSEN

- [1955] An isomorphism theorem for real closed fields, *Ann. of Math.*, Ser. 2, **61**, 542–554.

ERSHOV, Y.

- [1965] On the elementary theory of maximal normed fields, *Dokl. Akad. Nauk SSSR*, **165**. [English translation in *Sov. Math. Dokl.*, 1390–1393.]

GRATZER, G.

- [1968] *Universal Algebra* (Van Nostrand, New York).

HAUSDORFF, F.

- [1914] *Grundzüge der Mengenlehre* (Leipzig). [Reprinted by Chelsea, New York, 1955.]

HERMANN, G.

- [1926] Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.*, **95**, 736–788.

HERSTEIN, I.W.

- [1968] *Noncommutative Rings*, Carus Mathematical Monographs, No. 15 (Math. Assoc. Am., Buffalo, NY).

HIRSCHELMANN, A.

- [1972] An application of ultra-products to prime rings with polynomial identities, in: *Conference in Mathematical Logic — London '70*, Lecture Notes in Mathematics, Vol. 255 (Springer, Berlin) pp. 145–148.

KEGEL, O.H. and B.A.F. WEHRFRITZ

- [1973] *Locally Finite Groups* (North-Holland, Amsterdam).

KEISLER, H.J.

- [1964] Good ideals in fields of sets, *Ann. of Math.*, **79**, 338–359.
[1965] A survey of ultraproducts, in: *Logic, Methodology and Philosophy of Science*, edited by Y. Bar-Hillel (North-Holland, Amsterdam) pp. 112–126.

KOCHEN, S.

- [1961] Ultraproducts in the theory of models, *Ann. of Math.*, Ser. 2, **74**, 221–261.
[1975] The model theory of local fields, in: *Logic Conference Kiel 1974*, Lecture Notes in Mathematics, Vol. 499 (Springer, Berlin) pp. 384–425.

KÖNIG, J.

- [1903] *Einleitung in die allgemeine Theorie der algebraischen Grossen* (Teubner, Leipzig).

KUNEN, K.

- [1972] Ultrafilters and independent sets, *Trans. Am. Math. Soc.*, **172**, 299–306.

LANG, S.

- [1971] *Algebra* (Addison-Wesley, Reading, MA, revised printing).

ŁOŚ, J.

- [1955] Quelques remarques, theoremes et problemes sur les classes definissables d'algebres, in: *Mathematical Interpretation of Formal Systems* (North-Holland, Amsterdam) pp. 98–113.

MAL'CEV, A.I.

- [1940] On faithful representations of infinite groups of matrices *Mat. Sb.* **8**, 405–422.
[English translation in *Am. Math. Soc. Transl.* (2), **2** (1956) 1–21.]

NEUMANN, B.H.

- [1952] A note on algebraically closed groups, *J. London Math. Soc.* **22**, 247–249.

ROBINSON, A.

- [1975a] *Théorie Métamathématique des Idéaux*, Collection de Logique Mathématique, Ser. A (Paris–Louvain).
[1955b] On ordered fields and definite functions, *Math. Ann.*, **130**, 257–271.
[1962] A note on embedding problems, *Fund. Math.*, **50**, 455–461.
[1969] Problems and methods of model theory, in: *Aspects of Mathematical Logic*, C.I.M.E. 1968, III Ciclo (Edizioni Cremonese, Rome).
[1973a] On bounds in the theory of polynomials ideals, in: *Selected Questions of Algebra and Logic: Mal'cev memorial volume* (Novosibirsk) pp. 245–252.
[1973b] Model theory as a framework for algebra, in: *Studies in Model Theory*, edited by M. Morley, MAA Studies in Mathematics, Vol. 8 (Math. Assoc. Am., Buffalo, NY) pp. 134–157.

SABBAGH, G.

- [1969] How not to characterize the multiplicative groups of fields, *J. London Math. Soc.* (2), **1**, 369–370.

SEIDENBERG, A.

- [1971] On the length of a Hilbert ascending chain, *Proc. Am. Math. Soc.*, **29**, 443–450.
[1974] Constructions in algebra, *Trans. Am. Math. Soc.*, **197**, 273–313.

SHELAH, S.

- [1971] Every two elementarily equivalent models have isomorphic ultrapowers, *Israel J. Math.*, **10**, 224–233.

TERJANIAN, G.

- [1966] Un contre-exemple à une conjecture d'Artin, *C.R. Acad. Sci. Paris, Sér. A*, **262**, 612.

ZARISKI, O. and P. SAMUEL

- [1958] *Commutative Algebra* (Van Nostrand, New York).

Model Completeness

ANGUS MACINTYRE

Contents

Prologue	140
Introduction	140
1. Basic concepts and Robinson's Test	142
2. Applications: Nullstellensatz, Hilbert's 17-th Problem, Artin's Conjecture, and integral definite functions	146
3. The general theory: Model completions, existentially closed structures, and forcing.	154
4. Applications: Differentially closed fields and prime model extensions	164
5. Negative applications: Groups, skew fields, and number theories	167
6. Sheaves and model completeness	172
References	174

Prologue

Abraham Robinson created the theory of model completeness, and directed its growth for over 25 years. In this survey I will record the growth of the subject, with emphasis on interactions with algebra. This is for me a welcome chance to honor the memory of a unique mathematician, and a kind friend.

Introduction

I begin with some historical and methodological remarks.

The basic ideas of the subject can be located in the literature of the period 1950–1957. On the one hand, ROBINSON [1951, 1956] was at work on model completeness of specific algebraic examples. On the other hand, TARSKI and VAUGHT [1957] developed some fundamental results about elementary extensions (then called arithmetical extensions). I am not aware of any occurrence of the idea in earlier work, although there are obvious links with the Löwenheim–Skolem Theorem and Tarski’s quantifier elimination for real closed fields.

Why is it natural to study model completeness?

I think one can fairly say that elementary equivalence is the most fundamental concept in model theory. It is the analogue of isomorphism in general algebra. (One of the most striking results of the theory was the explication of elementary equivalence in terms of isomorphism of ultrapowers (SHELAH [1971])). By referring only to elementary equivalence and the “dual” concept of complete theory, one can formulate and obtain quite a few basic results, e.g. the Compactness Theorem, a weak Löwenheim–Skolem Theorem, and various important applications (for example, via ultraproducts, as in Chapter A.3). But already in the case of the Downward Löwenheim–Skolem Theorem, a close analysis would lead one to see that a stronger result was being proved, and that it was appropriate to introduce the notions of elementary substructure and elementary extension.

Again, model theory is a little older than category theory, and was certainly more subtle in 1950, but the subject could have benefited early on from a category-theoretic approach. This would inevitably have led one to elementary maps, of which elementary extensions are a special case.

It is in category-theoretic terms that one can best explain the advantages of introducing elementary maps. Tarski’s basic theorem (TARSKI and

VAUGHT [1957]) tells us that if L is a first order logic, then the category of L -structures with elementary maps has direct limits, and that the same holds for the subcategory of models of a fixed L -theory. Another desirable feature of the category and the above subcategories is the amalgamation property (see JONSSON [1965]). All this becomes relevant in obtaining the deeper results of the period 1955–present. These ideas show up in the study of homogeneous-universal models (see, e.g., CHANG and KEISLER [1973]), saturated models (CHANG and KEISLER [1973]), Morley theory (MORLEY [1965]), automorphisms and indiscernibles (GAIFMAN [1967]). The systematic use of Skolem functions in set theory (e.g. JENSEN [1972]) is a related phenomenon.

The final source of the idea, and the one most vital to Robinson, is the notion

relatively algebraically closed in,

coming from classical field theory. (Strictly speaking, a naive generalization of the above notion would give a concept weaker than $<$, because in the field theory case one was dealing with polynomials in one variable. But in interesting cases the two coincide.) Robinson abstracted from this source a notion of *model completion* of a theory, and proved that the model completion is unique if it exists. The canonical example was the theory of algebraically closed fields, as the completion of the theory of fields. The systematic use of these ideas by Robinson led to the nicest applications of model theory, to Hilbert's 17-th Problem (ROBINSON [1955]), and to Artin's Conjecture (AX and KOCHEN [1965a], ERSOV [1965]). AX's work (AX [1968]) on finite fields is also in this line of development. In another direction, Robinson's analysis led to remarkable progress in the study of differential fields (ROBINSON [1959a], SACKS [1972]). (It is however true to say that there are no *applications* of model completeness to problems in differential fields.)

Much later, in 1969, Robinson gave the general theory new vigor when he linked it with forcing (BARWISE and ROBINSON [1970], ROBINSON [1971]). In this way many new concepts appeared, and instruments for a finer analysis of previously intractable algebraic examples. New concepts of completion appeared, and some surprising connections with categoricity were established (SARACINO [1973]). The notion of existentially closed structure was rescued from obscurity (EKLOF and SABBAGH [1971]), and a satisfactory theory emerged.

The new applications can reasonably be described as negative results, in contrast to the work on Hilbert's 17-th Problem and Artin's Conjecture.

That is, the new results typically showed that some natural structures are extremely complicated (MACINTYRE [1972], HIRSCHFELD and WHEELER [1975]). But unquestionably the algebra and Robinson's methods work nicely together.

The final development to be discussed here is the connection between sheaves and model completeness results in ring theory. Here, a positive result of LIPSHITZ and SARACINO [1973] and CARSON [1973] inspired a transfer theorem (MACINTYRE [1973a], WEISSPFENNING [1973]). From this one can obtain an analogue of Hilbert's 17-th Problem for real regular rings.

The main topic omitted because of lack of space is the study of hierarchies for existentially closed structures, and the resulting definition of generic structures without using forcing (SIMMONS [1972b], [1973b], HENRARD [1973]). This work is important, but has not till now made contact with algebra.

1. Basic concepts and Robinson's Test

1.1. For the basic concepts of first order logic, I refer to Chapters A.1 and A.2. For material on ultraproducts, see Chapter A.3.

I wish to keep notation as informal as possible, so, for example, I make no notational distinction between a structure and its underlying set. $\mathbf{m}$ will be a finite tuple $\langle m_1, \dots, m_k \rangle$, and if f is a map defined on each m_i , then $f(\mathbf{m})$ will be $\langle f(m_1), \dots, f(m_k) \rangle$. If c is an L-constant, $c^{\mathfrak{M}}$ is the interpretation of c in $\mathfrak{M}$.

1.2. Let L be a first order language. I associate with L a category $\mathcal{C}_L$ of L-structures. The objects of $\mathcal{C}_L$ are the L-structures. The morphisms of $\mathcal{C}_L$ are the monomorphisms of L-structures. That is, a map $f: \mathfrak{M} \rightarrow \mathfrak{N}$ is a morphism iff

(i) for each individual constant c of L, $f(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$, and

(ii) for each *atomic* L-formula φ , and tuple $\mathbf{m}$ from $\mathfrak{M}$,

(*) $\mathfrak{M} \models \varphi(\mathbf{m})$ iff $\mathfrak{N} \models \varphi(f(\mathbf{m}))$.

Obviously we get a category $\mathcal{C}_L$ in this way. Obviously $\mathcal{C}_L$ has direct limits.

If T is any L-theory, we have a corresponding subcategory $\mathcal{C}_T$, whose objects are the models of T . (Such a class is called an EC_Δ class.) $\mathcal{C}_T$ may not have direct limits. An easy example is got by taking T as the theory of ordered sets with first element. In fact, by the Chang-Łoś-Susko Theorem (ROBINSON [1963]), $\mathcal{C}_T$ has direct limits iff T is an $\forall\exists$ theory.

A morphism f is *elementary* if $(*)$ holds for *all* formulas φ . Let $\mathcal{C}_L^<$ be the category consisting of L -structures with elementary maps, and let $\mathcal{C}_T^<$ be the corresponding category of models of T . The most fundamental fact is:

THEOREM 1 (TARSKI and VAUGHT [1957]). $\mathcal{C}_L^<$ has direct limits

COROLLARY. $\mathcal{C}_T^<$ has direct limits.

In plainer terms, the union of an elementary chain is an elementary extension of each member of the chain.

Note. The preceding ideas and results go through in quite a wide setting. For example, the concepts, examples, and results all work for $L_{\infty, \omega}$. The concept makes good sense for $L(Q)$, Q a cardinality quantifier (see 5.5 of Chapter A.1) but the Tarski result would go through only for long chains. In general what is needed is a logic with securable or continuous quantifiers (MAKOWSKY [1973]). The Tarski proof has nothing to do with compactness.

1.3. We come now to another category-theoretic property of $<$, which this time does depend on compactness. The proof of Theorem 2 is a simple application of the Compactness Theorem (see 2.4 of Chapter A.1), and can be found in SIMMONS [1972a].

THEOREM 2. Suppose L is a first order language, and $\mathfrak{A}, \mathfrak{M}, \mathfrak{N}$ are L -structures. Given morphisms

$$\begin{array}{ccc} \mathfrak{A} & \longrightarrow & \mathfrak{M} \\ \downarrow & & \\ \mathfrak{N} & & \end{array}$$

in $\mathcal{C}_L^<$, we can complete the diagram to a commuting square in $\mathcal{C}_L^<$.

Note that I do not claim that pushouts exist. But we can improve Theorem 2 a little, as Bacsich and Fisher showed me in 1971. Namely, in completing the above diagram, we can insist that $f(m) \neq g(n)$ unless $m = n \in \mathfrak{A}$. See BACSICH and ROWLAND-HUGHES [1974].

1.4. There is an interesting characterization of elementary maps in terms of ultrapowers. This comes from the Keisler–Shelah Theorem (CHANG and KEISLER [1973], SHELAH [1971]).

THEOREM 3. $f: \mathfrak{M} \rightarrow \mathfrak{N}$ is elementary iff there exists an index set I , an ultrafilter D on I , and an isomorphism

$$g: \mathfrak{M}^I/D \leftrightarrow \mathfrak{N}^I/D$$

such that the diagram

$$\begin{array}{ccc} \mathfrak{M} & \xrightarrow{f} & \mathfrak{N} \\ \Delta \downarrow & & \downarrow \Delta \\ \mathfrak{M}^I/D & \xrightarrow{g} & \mathfrak{N}^I/D \end{array}$$

commutes, where the Δ are the natural diagonal embeddings.

1.5. Before arriving at the notion of model completeness, I have to introduce some weakenings of $<$.

DEFINITION. $f: \mathfrak{M} \rightarrow \mathfrak{N}$ is an $\forall_n$ -map also written:

$$\mathfrak{M} \xrightarrow[\prec_n]{f} \mathfrak{N},$$

iff (*) of 1.2 holds for all formulas φ which are prenex with at most n alternations of quantifiers, and with leading quantifier $\forall$.

So $<_0$ corresponds to *embedding*, and $<_1$ is a natural generalization of *relatively algebraically closed in*. Obviously, f is elementary iff f is $\forall_n$ for each n . Now I state a key result.

LEMMA 4 (CHANG and KEISLER [1973]). $f: \mathfrak{M} \rightarrow \mathfrak{N}$ is $\forall_1$ if and only if there exists an embedding $g: \mathfrak{N} \rightarrow \mathfrak{M}^*$ such that $g \circ f$ is elementary.

The proof is a routine compactness argument. $\mathfrak{M}^*$ can be chosen as an ultrapower of $\mathfrak{M}$, and $g \circ f$ as the diagonal map.

1.6. DEFINITION. T is *model complete* iff every embedding ($\forall_0$ -map) in $\mathcal{C}_T^{\preceq}$ is elementary.

The next theorem is geared to applications.

THEOREM 5 (Robinson's Test). *A theory T is model complete if and only if every embedding in $\mathcal{C}_T$ is $\forall_1$.*

PROOF. I give the proof mainly because it uses the method of alternating chains, which is the main method of the general theory.

The proof of $(\Rightarrow)$ is clear. To prove $(\Leftarrow)$, suppose that $\mathfrak{M} \rightarrow \mathfrak{N}$ is an embedding in $\mathcal{C}_T$. So it is $\forall_1$. By Lemma 4, I get

$$\begin{array}{ccccc} \mathfrak{M} & \xrightarrow{\leq_1} & \mathfrak{N} & \xrightarrow{\leq_0} & \mathfrak{M}_1 \\ & \searrow & & \nearrow & \\ & & \mathfrak{N} & & \end{array}$$

commuting. Of course, $\mathfrak{M}_1 \models T$, so I do the same for the pair $\mathfrak{N}, \mathfrak{M}_1$, to get

$$\begin{array}{ccccccc} \mathfrak{M} & \xrightarrow{\leq_1} & \mathfrak{N} & \xrightarrow{\leq_0} & \mathfrak{M}_1 & \xrightarrow{\leq_0} & \mathfrak{N}_1 \\ & \searrow & & \nearrow & & \nearrow & \\ & & \mathfrak{N} & & \mathfrak{M}_1 & & \mathfrak{N}_1 \end{array}$$

Proceeding in this way I construct $\mathfrak{M}_k, \mathfrak{N}_k$ with

$$\mathfrak{M} \rightarrow \mathfrak{N} \rightarrow \mathfrak{M}_1 \rightarrow \mathfrak{N}_1 \rightarrow \cdots \rightarrow \mathfrak{M}_k \rightarrow \mathfrak{N}_k \rightarrow \mathfrak{M}_{k+1} \rightarrow \mathfrak{N}_{k+1} \cdots,$$

where the diagram commutes, and where $\mathfrak{M} \rightarrow \mathfrak{M}_1$, $\mathfrak{N} \rightarrow \mathfrak{N}_1$, $\mathfrak{M}_k \rightarrow \mathfrak{M}_{k+1}$, $\mathfrak{N}_k \rightarrow \mathfrak{N}_{k+1}$ are all elementary. Form $\varinjlim \mathfrak{M}_k = \varinjlim \mathfrak{N}_k = \mathfrak{A}$, say. Then by Tarski, the natural maps

$$\mathfrak{M} \rightarrow \mathfrak{A}, \quad \mathfrak{N} \rightarrow \mathfrak{A}$$

are elementary, whence $\mathfrak{M} \rightarrow \mathfrak{N}$ is elementary. Therefore T is model complete. $\square$

1.7. In first applications, model completeness was used mainly as a tool to prove completeness, by using the Prime Model Test, whose proof is obvious.

THEOREM 6 (Prime Model Test). *If T is model complete, and there is a model $\mathfrak{M}$ of T embeddable in all models of T , then T is complete.*

Example. T = theory of algebraically closed fields of characteristic 0. $\mathfrak{M}$ is the field of real algebraic numbers. Theorem 7 will tell us that T is model complete. So T is complete.

1.8. Robinson's Test is of great practical value, as I shall indicate later. By trivial reductions, the test comes down to showing that embeddings respect formulas $\forall y A(v, y)$, where A is a conjunction of atomic formulas and their negations. That is, if $\mathfrak{M} \subseteq \mathfrak{N}$, $\mathfrak{M}, \mathfrak{N}$ models of the theory in question, and $\mathfrak{M} \models \forall y A(m, y)$, then $\mathfrak{N} \models \forall y A(m, y)$, whenever m is a tuple from $\mathfrak{M}$.

2. Applications: Nullstellensatz, Hilbert's 17-th Problem, Artin's Conjecture, and integral definite functions

2.1. I wish to follow as much as possible the historical development of the subject. The main applications followed the material of Section 1, and were carried out between 1950 and 1970. After 1970 we entered a new period of theoretical development, whose applications (to be given in Section 5) have a different character.

The applications in this section are to field theory. The inspiration is Robinson's. What must we know to apply Robinson's Test?

Let T be a theory of fields. We have to know that if $\mathcal{M}, \mathcal{N} \models T$, $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{M} <_1 \mathcal{N}$. By the reduction mentioned earlier, we must show: If Σ is a finite system of equations and inequations over $\mathcal{M}$ (i.e. with parameters from $\mathcal{M}$), and Σ is solvable in $\mathcal{N}$, then Σ is solvable in $\mathcal{M}$.

In field theory, inequations can be replaced by equations, because of the equivalence

$$a \neq 0 \Leftrightarrow \exists y (a \cdot y = 1),$$

so we may assume Σ is a system of equations. But then our condition on Σ begins to look like a Nullstellensatz, and Robinson liked and pursued this analogy. A *weak* version of Hilbert's Nullstellensatz (LANG [1958]) says:

If $\mathcal{M}$ is algebraically closed, and Σ has a solution in $\mathcal{N}$, then Σ has a solution in $\mathcal{M}$.

But this is just the data needed to apply Robinson's Test. So from the Nullstellensatz we can derive the model completeness of the theory of algebraically closed fields. This result was first obtained by TARSKI [1951] by quantifier elimination. Tarski did not use the Nullstellensatz.

Conversely, we can always derive a Nullstellensatz for any model complete theory of fields. So in particular the Nullstellensatz given above for algebraically closed fields follows from Tarski's analysis.

ROBINSON [1951] also found a model completeness proof independent of the Nullstellensatz, and this style of proof became very popular. His proof goes thus. Suppose $\mathcal{M} \subseteq \mathcal{N}$, where $\mathcal{M}, \mathcal{N}$ are algebraically closed fields, and not $\mathcal{M} <_1 \mathcal{N}$. Without loss of generality (because we are dealing with failure of $\forall_1$ -extensions) $\mathcal{N}$ has finite transcendence degree over $\mathcal{M}$, and so without loss of generality $\mathcal{N}$ has transcendence degree 1 over $\mathcal{M}$. Let $\{t\}$ be a transcendence base for $\mathcal{N}$ over $\mathcal{M}$. By the assumption that not $\mathcal{M} <_1 \mathcal{N}$, there is a quantifier-free formula φ , and tuple m from $\mathcal{M}$ such that $\mathcal{N} \models \exists v \varphi(v, m)$ but $\mathcal{M} \models \neg \exists v \varphi(v, m)$. Robinson made the basic observation that

(S) $\text{Diagram}(\mathfrak{M}(t)) \cup \text{Theory of algebraically closed fields} \vdash \exists v \varphi(v, m)$.

(S) follows from Steinitz's Theorem (JACOBSON [1964]) that there is a prime algebraically closed field containing $\mathfrak{M}(t)$, namely $\mathfrak{N}$. But from (S) by the Compactness Theorem one easily deduces that

$$\mathfrak{M} \models \exists v \varphi(v, m).$$

See ROBINSON [1963] for a full proof.

So we see that from Steinitz we can deduce a Nullstellensatz.

To summarize this subsection, let me say that we have proved:

THEOREM 7. *The theory of algebraically closed fields is model complete.*

We have outlined several approaches, and stressed the link to the Nullstellensatz. There are other proofs. One can use Steinitz and Theorem 3. One can use Steinitz and Lindstrom's Theorem (see Section 3).

2.2. Robinson then applied his method to real closed fields (ROBINSON [1955]). In this case there is no familiar Nullstellensatz. However, using Tarski's quantifier elimination method, one can obtain:

THEOREM 8. *The theory of real closed ordered fields is model complete.*

So one can deduce a Nullstellensatz, but this seems to have no special importance. For a proof of quantifier elimination see TARSKI [1951], or better, COHEN [1969].

Robinson obtained model completeness by using two facts, namely:

I. There is a prime real closed extension of any ordered field.

II. If K is real closed, then $K(x)$ is determined as an ordered field by the cut x makes in K .

His proof then goes smoothly along the lines of his proof for algebraically closed fields. (At the end one must use the trivial fact that ordered fields are densely ordered without last element.)

Robinson's proof does not give quantifier elimination directly. To supplement his treatment one would have to rely on his theorem (to be explained in Section 3) that the model completion of a universal theory has elimination of quantifiers.

There is a later proof due to KOCHEN [1961], by the ultraproduct method. Essentially, one identifies the $\aleph_1$ -saturated real closed fields and proves an

isomorphism theorem from which model completeness follows. This proof uses the same facts Robinson used. One can also obtain quantifier-elimination thus, using an observation of SHOENFIELD [1971], or BLUM [1968].

(It should be clear that the methods are in some sense equivalent. This is obvious in the classical algebraic examples. But I wish to remark that there are instructive cases (ROBINSON [1959b], ERSOV [1967]) where Kochen's method seems easier than Robinson's, and vice versa.)

2.3. Hilbert's 17-th Problem

Now I come to a genuine application. The problem was: Suppose f is a positive definite rational function in $x_1, \dots, x_n$ over $\mathbb{Q}$, or $\mathbb{R}$. Is f necessarily a sum of squares of rational functions?

The problem was solved affirmatively by Artin in 1927 (ARTIN and SCHREIER [1926], ARTIN [1927]). To do this, they invented the theory of real closed fields, and proved the fundamental facts on existence and uniqueness of real closure. The main idea is a generalization of Sturm's Theorem (JACOBSON [1964]). It seems that no existing treatment, whether by logic or algebra, has avoided the use of Sturm's Theorem. (The attempt to do so has led to serious errors in both camps.) Of course, COHEN [1969] gets by without making Sturm's Theorem explicit (he uses the so-called Sign Change Property instead). But there is no known way to get directly from Cohen's result to the theoretical facts needed for Hilbert's 17-th Problem. (There was a beguiling possibility of using results of Morley–Shelah type (SACKS [1972]), on prime model extensions, to bridge the gap. But it seems that to verify the hypotheses of such theorems one needs Sturm's Theorem.)

Let us therefore assume the basic facts on existence of real closure. The logic proof will be shorter and more perspicuous than any proof disdaining the use of logic. (It is noteworthy that Jacobson's new algebra text (JACOBSON [1974]) uses the logic approach to real closed fields.)

I now give Robinson's solution of Hilbert's 17-th Problem. Let K be an ordered field, with a unique ordering ($\mathbb{Q}$, $\mathbb{R}$ are such fields). Suppose $f \in K(x_1, \dots, x_n)$, and f is not a sum of squares. By a beautiful argument having nothing to do with logic, Artin and Schreier showed that $K(x_1, \dots, x_n)$ may be ordered so that $f < 0$. K is a subfield of $K(x_1, \dots, x_n)$, so K inherits an order from $K(x_1, \dots, x_n)$. By uniqueness this must be the original order on K . By the general theory we have a commuting diagram of embeddings

$$\begin{array}{ccc}
 K & \xrightarrow{\quad} & K(x_1, \dots, x_n) \\
 \downarrow & & \downarrow \\
 \text{Real closure} & \xrightarrow{\quad} & \text{Real closure of} \\
 \text{of } K & & K(x_1, \dots, x_n)
 \end{array}$$

But $f < 0$ in $K(x_1, \dots, x_n)$, and so $f < 0$ in the real closure of $K(x_1, \dots, x_n)$. So the real closure of $K(x_1, \dots, x_n)$ satisfies $\exists x_1 \cdots \exists x_n [f(x_1, \dots, x_n) < 0]$. By model completeness, the real closure of K also satisfies $\exists x_1 \cdots \exists x_n [f(x_1, \dots, x_n) < 0]$. Assume now that K is dense in the real closure of K . Then

$$K \models \exists x_1 \cdots \exists x_n [f(x_1, \dots, x_n) < 0].$$

So f is not positive definite.

We have answered the Hilbert problem affirmatively for fields K which have a unique order and are dense in their real closure. Of course, $\mathbb{Q}$ and $\mathbb{R}$ are such fields. Recently, McKenna [1975] building on work of Scott [1969] obtained the nice result that if K has a unique order, then Hilbert's 17-th Problem has an affirmative answer for K if and only if K is dense in its real closure.

Robinson's work described above remains one of the very best applications of logic to algebra. Till now, it has been surpassed only by the work of Ax-Kochen and Ersov on p -adic fields and Artin's Conjecture. Clearly, Robinson's work inspired the later achievements.

2.4. Artin's Conjecture

After the above work one has quite a clear project for future progress. The delay of one decade before progress was made can be explained neatly by a remark of Blum [1968]. Robinson's application was "after the algebraic facts" — the work on p -adic fields would *establish* fundamentally important algebraic results. Accordingly, it required extensive algebraic preliminaries.

It was natural to expect that the model theory of p -adic fields would resemble that of real fields. The most obvious similarities are

- (a) both $\mathbb{R}$ and $\mathbb{Q}_p$ are locally compact fields;
- (b) for both $\mathbb{R}$ and $\mathbb{Q}_p$ we have a viable topological-algebraic criterion enabling us to locate zeros of polynomials, namely, for $\mathbb{R}$ the Sign Change Property or Sturm's Theorem, and for $\mathbb{Q}_p$ Hensel's Lemma (JACOBSON [1964]) or variants.

Of course, (b) is of most importance, since this type of result for real closed fields is the cornerstone of the whole algebraic and logical theory. So

our project should be to find p -adic analogues of *ordered field* and *real closed field*, and to prove analogues of Facts I and II of 2.2, taking Hensel's Lemma as our key idea.

This is precisely what was done in the great advances made by Ax and KOCHEN [1965a, 1965b, 1966] and ERSOV [1965] from 1964 onwards. As in the case of Hilbert's 17-th Problem, a remarkable feature of the method is that to prove an algebraic result about an individual field one has to prove model theoretic results about certain elementary classes containing this field. I will not enter into details. The main complications are algebraic, and model theory guides us through these complications. For the full story one can consult the above-cited papers.

General setting. L is the natural language for valued fields. $\mathcal{F}$ is a class of fields, and Γ a class of ordered abelian groups. $\mathcal{U}(\mathcal{F}, \Gamma)$ is the class of valued fields whose value group is in Γ and whose residue class field is in $\mathcal{F}$. $\mathcal{U}_H(\mathcal{F}, \Gamma)$ is the subclass of $\mathcal{U}(\mathcal{F}, \Gamma)$ consisting of the fields that satisfy Hensel's Lemma. Obviously, if $\mathcal{F}, \Gamma$ are EC_Δ -classes so is $\mathcal{U}_H(\mathcal{F}, \Gamma)$.

The theorem with the deepest application is:

THEOREM 9. *Suppose $\mathcal{F}$ and Γ are EC_Δ classes, each with complete theory. Suppose all members of $\mathcal{F}$ have characteristic 0. Then $\mathcal{U}_H(\mathcal{F}, \Gamma)$ has complete theory.*

This is not a model completeness result, though intimately related to such results. The algebraic analysis goes thus:

(a) Show that every member of $\mathcal{U}(\mathcal{F}, \Gamma)$ has a unique *immediate* (KAPLANSKY [1942]) algebraic extension to a member of $\mathcal{U}_H(\mathcal{F}, \Gamma)$. This depends on the characteristic 0 assumption. This gives us the analogue of real closure.

(b) Establish an analogue of Fact II of 2.2.

There are various auxiliary complications, which we ignore here. Then the theorem is readily proved by ultraproducts or saturated models.

Application of Theorem 9. For prime p , let $\mathbb{F}_p((t))$ be the field of formal Laurent series over the finite field $\mathbb{F}_p$. This is of course a valued field with residue class $\mathbb{F}_p$ and value group $\mathbb{Z}$. It satisfies Hensel's Lemma. Most importantly, it is a C_2 field, as proved by LANG [1952].

Let D be a non-principal ultrafilter on the set P of primes. Form $\prod_{p \in P} \mathbb{F}_p((t))/D$. This is a valued field, with residue class field $\prod_{p \in P} \mathbb{F}_p/D$, and value group $\mathbb{Z}^P/D$. It also satisfies Hensel's Lemma, and is C_2 , by the Fundamental Theorem on ultraproducts. *Its residue class field has characteristic 0.*

Form $\prod_{p \in P} \mathbf{Q}_p / D$. This has the same residue class field and value group as the above ultraproduct, and it satisfies Hensel's Lemma. By Theorem 9,

$$\prod_{p \in P} \mathbb{F}_p((t)) / D \equiv \prod_{p \in P} \mathbf{Q}_p / D,$$

so $\prod_{p \in P} \mathbf{Q}_p / D$ is C_2 .

In some sense this says that the average $\mathbf{Q}_p$ is C_2 . Artin's famous conjecture said that each $\mathbf{Q}_p$ is C_2 . From logic we get: For each n, d there is a prime $q(n, d)$ such that if $p > q(n, d)$ and f is a homogeneous polynomial over $\mathbf{Q}_p$ in n variables and of degree d , and if $n > d^2$, then f has a non-trivial zero in $\mathbf{Q}_p$.

This turned out (TERJANIAN [1966]) to be the best possible result.

We should note that COHEN [1969] has a nice proof, along the lines of Tarski's work on real closed fields.

ERSOV [1965] gives various interesting extensions of these methods to the study of C_i fields.

2.5. Model completeness of $\mathbf{Q}_p$

We now face a slightly different situation. $\mathbf{Q}_p$ has finite residue class field, although $\mathbf{Q}_p$ itself is of characteristic 0. To obtain (a) for Theorem 9, one used work of KAPLANSKY [1942]. This does not apply to $\mathbf{Q}_p$ and the fields elementarily equivalent to it.

Let $\mathcal{F}$ be the class $\{\mathbb{F}_p\}$, and Γ the class of $\mathbb{Z}$ -groups (the class of groups elementarily equivalent to $\mathbb{Z}$ (PRESBURGER [1929]); this class is model complete if we distinguish the least positive element 1). Then $\mathbf{Q}_p$ is in $\mathcal{U}_H(\mathcal{F}, \Gamma)$. But so is $\mathbb{F}_p((t))$, and this is clearly not elementarily equivalent to $\mathbf{Q}_p$. We distinguish the two by the sentence

$$v(p) = 1,$$

true in $\mathbf{Q}_p$, false in $\mathbb{F}_p((t))$.

Let $\mathcal{U}_H^*(\mathcal{F}, \Gamma)$ be the subclass of $\mathcal{U}_H(\mathcal{F}, \Gamma)$ satisfying the above sentence. $\mathcal{U}_H^*(\mathcal{F}, \Gamma)$ is EC_Δ whenever $\mathcal{F}$ and Γ are.

THEOREM 10 (AX and KOCHEN [1966], ERSOV [1965]). *Let $\mathcal{F} = \{\mathbb{F}_p\}$, and let Γ be the class of $\mathbb{Z}$ groups. Then the theory of $\mathcal{U}_H^*(\mathcal{F}, \Gamma)$ is complete and model complete.*

There are several variants of the proof. I feel that the proof of ERSOV [1965] via Robinson's Test is rather natural. The original proofs used the extraneous notion of *cross-section* (AX and KOCHEN [1966]), and were

more complicated than need be. Cohen's proof [1969], which is very elegant and direct, gives quantifier elimination for $\mathbf{Q}_p$, using the cross-section $n \rightarrow p^n$.

The approach for the model-theoretic proofs is like that for Theorem 9. One establishes analogues of (a) and (b). This time one has to invent the algebra first (AX and KOCHEN [1965b], Lemma 8).

The quantifier-elimination problem for $\mathcal{U}_H^*(\mathcal{F}, \Gamma)$ is rather interesting. If one brings the cross-section into the formal language then one has elimination of quantifiers (AX and KOCHEN [1966], COHEN [1969], WEISSPFENNING [1971].) This can be done constructively or by the Shoenfield criterion cited in 3.2. But then it is very hard to figure out what are the definable subsets of $\mathbf{Q}_p$. This contrasts with the case of $\mathbb{R}$, where TARSKI [1951] gave a perspicuous and useful description of the definable sets. With this in mind, I gave (MACINTYRE [1974a]) a reformulation of the whole theory, in terms of predicates for the valuation ring and the sets of n -th powers, under which $\mathbf{Q}_p$ has elimination of quantifiers. We then have the following:

THEOREM 11 ($K = \mathbb{R}$ or $\mathbf{Q}_p$). *Any infinite definable subset of K has non-empty interior.*

One may speculate also that this approach will give us explicitly a p -adic analogue of Sturm's Theorem.

2.6. The analogue of Hilbert's 17-th Problem

Now that we have model completeness for $\mathbf{Q}_p$, and the relevant facts about prime model extension, we can hope to get results like those in 2.3. Well, we need analogues of:

- (i) positive definite,
- (ii) sum of squares.

An analogue of (i) comes to mind, namely integral definite. Suppose $f \in \mathbf{Q}_p(x_1, \dots, x_n)$. f is integral definite if $v(f(\alpha_1, \dots, \alpha_n)) \geq 0$ whenever $v(\alpha_i) \geq 0$ for $1 \leq i \leq n$.

An analogue of (ii) is less obvious, and was found by KOCHEN [1969]. He then modified each step of Robinson's analysis, and obtained a remarkable analogue of the solution of Hilbert's 17-th Problem. The result is too complex to be stated compactly, so we recommend the reader to go to Kochen's paper. There is some possibility that Kochen's analysis may enable us to understand the nature of the counterexamples to Artin's Conjecture (TERJANIAN [1966]).

2.7. There are many other model completeness results along the lines of Theorem 10. The interested reader should look at Ersov's paper (ERSOV [1965]), as well as ZIEGLER [1972].

2.8. There is an intriguing open problem in this area.

Problem. What is the elementary theory of $\mathbb{F}_p((t))$?

The obstruction to progress is that we know no analogue of the (a), (b) of 2.4. The only result in this direction is to be found in COVEN [1972], using a result from Greenberg [1969].

2.9. Separably closed fields

A field K is separably closed if it has no separable algebraic extensions. ERSOV [1967] classified the elementary types of separably closed fields, by using Robinson's Test.

The key algebraic result needed (as we might expect) is a Nullstellensatz. This can be found in LANG [1958]. As far as I know, there are no applications of Ersov's result. Further, no other proof has been obtained which might imply the relevant Nullstellensatz.

2.10. Finite fields

In 1967–1968 (Ax [1968]), Ax succeeded in analyzing the model theory of finite fields, and thereby solved positively the old problem of the decidability of finite fields. Ax's original method of proof was by saturated models, but as usual the main ideas are those needed for a proof in the style of Robinson's Test.

Ax essentially had to find axioms for ultraproducts of finite fields. The relevant axioms for such fields K are:

- (i) K is perfect,
 - (ii) K has exactly one extension of each degree;
- and the all important
- (iii) every absolutely irreducible variety over K has a point in K .
- Axiom (iii) is deep. Note that of course (iii) is a sort of Nullstellensatz. On formal grounds one can expect (iii) to imply a weak form of model completeness.

Ax found elementary invariants for the fields (so-called pseudofinite fields) satisfying (i)–(iii). Later his students ADLER and KIEFE [1976] found model completeness results (indeed quantifier elimination) for such fields, at the cost of adding some auxiliary predicates to the language.

Recently, JARDEN and KIEHNE [1975] simplified Ax's treatment, and extended his results.

Again, there seems to be till now no application of Ax's brilliant analysis. In Theorem 8.10 of Chapter A.3 there is a nice result which turned up in the course of Ax's work.

2.11. Decidability

In all the above cases, one obtained decidability results by general nonsense once one had explicit axiomatizations. In all cases but 2.9 and 2.10 primitive recursive procedures are known (COHEN [1969]), and for finite fields such a procedure has been announced (FRIED and SACERDOTE [1975]). Moreover, the model-theoretic approach enables one to obtain effective bounds in the theory of polynomial ideals. For more on this see Chapter A.3.

3. The general theory: Model completions, existentially closed structures, and forcing

3.1. Early on, Robinson discerned a general pattern in the preceding examples. He isolated the notion of *model completion* of a theory, and proved some satisfying general results. Since 1970, largely due to the efforts of Robinson, his students, and associates, the general theory has been much refined, making possible new sorts of applications to algebra.

3.2. Model completion

This is a sort of dual to the operation which assigns to a field (resp. an ordered field) its algebraic closure (resp. its real closure).

DEFINITION. Let T, T^* be L -theories. T^* is a *model completion* of T iff

- (a) T and T^* are mutually model consistent, i.e. every model of T is embeddable in a model of T^* and vice versa;
- (b) T^* is model complete;
- (c) If $\mathcal{M} \models T$, then $T^* \cup \text{Diagram}(\mathcal{M})$ is complete.

A moment's reflection shows that clause (c) is related to the uniqueness of algebraic closure. Namely, it says that a model of T is embeddable in a model of T^* "in a unique way" (cf. fact I of 2.2).

In time, around 1970, a weaker notion appeared. T^* is a *model companion* of T if (a) and (b) hold.

Example 1. T = theory of fields. T^* = theory of algebraically closed

fields. That T^* is a model completion of T follows from quantifier elimination for T^*

Example 2. T = theory of ordered fields. T^* = theory of real closed fields. That T^* is a model completion of T follows from quantifier elimination for real closed ordered fields.

Example 3. T = theory of formally real fields. (No symbol for $<$.) T^* = theory of real closed fields. T^* is a model companion for T , but not a model completion (EKLOF and SABBAGH [1971]). The reason is that we do not have quantifier elimination for real closed fields unless we allow *order* as a primitive notion.

Example 4 (Needed later). T = theory of Boolean algebras. T^* = theory of atomless Boolean algebras. T^* is a model completion of T .

Example 3 suggests the easy:

LEMMA 12. (a) *Suppose T^* is a model companion of T , where T is a universal theory. Then T^* is a model completion of T if and only if T^* has elimination of quantifiers.*

(b) *Suppose T^* is a model companion of T . Then T^* is a model completion of T if and only if T has the amalgamation property.*

The proof is related to Shoenfield's criterion (SHOENFIELD [1971]).

3.3. The most important early result was:

THEOREM 12 (ROBINSON [1963]). *A theory T has at most one model companion.*

The proof is by an alternating chains argument. I will shortly give a modern version of the argument, due to SIMMONS [1975]. But first we should observe that a theory may have no model companion. We will see interesting examples later.

I write T^* for the model companion of T , when this exists.

What are the obvious properties of the partial map $T \mapsto T^*$?

For any T , let $T_{\forall}$ (resp. $T_{\forall\exists}$) be the theory whose axioms are the universal (resp. universal existential) consequences of T . By using the

theorems of Łoś–Tarski (ROBINSON [1963]) and Chang–Łoś–Suszko (ROBINSON [1963]), which are discussed in Chapter A.2, we easily get:

- (i) If T^* is defined, so is $(T_v)^*$, and $T^* = (T_v)^*$.
- (ii) If $(T_v)^*$ is defined, so is T^* , and $T^* = (T_v)^*$.
- (iii) T^* is an $\forall\exists$ theory, and $T_{\forall\exists} \subseteq T^*$.

Results (i) and (ii) correspond to (a) of 3.1, and (iii) corresponds to (b).

Note the obvious

LEMMA 13. *If T is model complete, then T is $\forall\exists$.*

(This is immediate from the direct limit theorem, and the Chang–Łoś–Suszko theorem.)

Note also that there are complete $\forall\exists$ theories which are not model complete. The most natural example I know is the theory of algebraically closed fields of fixed characteristic, with distinguished proper algebraically closed subfield (ROBINSON [1959b]). By (iii) this theory has no model companion.

Now I go back to consider the map $T \mapsto T^*$. A remarkable development after 1969 was the following: Various constructions were found giving *total* maps $T \rightarrow T^*$ which extend $T \mapsto T^*$.

DEFINITION. An operation $T \mapsto T^*$ on theories is a *companion operator* if

- (i) $(T^*)_v = T_v$;
- (ii) if $T_v = T'_v$, then $T^* = (T')^*$;
- (iii) $T_{\forall\exists} \subseteq T^*$.

It turns out that there are many interesting companion operators. But:

THEOREM 14. *Suppose $\#$ is a companion operator. Suppose T has a model companion T^* . Then $T^* = T^\#$.*

PROOF. $T_v = (T^*)_v$. Thus $T^\# = (T^*)^\# \supseteq (T^*)_{\forall\exists} = T^*$, so

$$T^* \subseteq T^\#. \quad (1)$$

Note that here I don't use model completeness of T^* , only that T^* is $\forall\exists$, to obtain (1)

Now, suppose $\mathcal{M} \models T^*$. Using the mutual model consistency of T , T^* and $T^\#$, one gets a chain

$$\mathcal{M} = \mathcal{M}_0 \subseteq \mathcal{M}_1 \subseteq \mathcal{M}_2 \subseteq \cdots$$

with $\mathfrak{M}_\infty = \lim \mathfrak{M}_n$, where $\mathfrak{M}_{2n} \models T^*$, and $\mathfrak{M}_{2n+1} \models T^*$. By Chang–Łos–Suszko, $\lim \mathfrak{M}_{2n+1} \models (T^*)_{\forall\exists}$, so $\mathfrak{M}_\infty \models (T^*)_{\forall\exists}$. But by model completeness of T^* ,

$$\mathfrak{M} = \mathfrak{M}_0 < \lim_{\rightarrow} \mathfrak{M}_{2n} = \mathfrak{M}_\infty. \quad \text{Thus } \mathfrak{M} = (T^*)_{\forall\exists}.$$

Since $\mathfrak{M}$ was arbitrary,

$$(T^*)_{\forall\exists} \subseteq T^*. \quad (2)$$

So,

$$(T^*)_{\forall\exists} \subseteq T^* \subseteq T^*.$$

Since T^* is $\forall\exists$, it follows that $(T^*)_{\forall\exists} = T^*$.

Finally, it follows that T^* is model complete, since T^* is, so $(T^*)_{\forall\exists} = T^*$, so $T^* = T^*$ $\square$

Theorem 12 would be an immediate corollary, if we knew just one companion operator. I now give some examples, so we have Theorem 12.

Examples of companion operators

Example 1. Kaiser Hull. By (1) of the preceding proof, we see that if T' is $\forall\exists$ and mutually model consistent with T , then $T' \subseteq T^*$. This suggests the existence of a minimal companion operator, perhaps the maximal $\forall\exists$ theory mutually model consistent with T . Why does such exist? $T_{\forall\exists}$ is mutually model consistent with T , and if T_1, T_2 are then so is $T_1 \cup T_2$. This is proved by the ubiquitous alternating chains argument (KAISER [1969]). So we get T^0 , the Kaiser Hull of T , and $T \mapsto T^0$ is obviously a companion operator. For a while it was the only one known. Notice how natural it is. An $\forall\exists$ sentence tells us, typically, conditions under which a system has a solution, surely the sort of thing one would want as an axiom for *closed* structures.

This brings us to existentially closed structures and:

Example 2. The operator $T \mapsto T^e$

DEFINITION. Suppose $M \models T_\forall$. $\mathfrak{M}$ is *T-existentially closed* (*T-e.c.*) if $\mathfrak{M} \subseteq M_1 \models T_\forall$ implies $\mathfrak{M} <_1 M_1$.

Universal algebraic arguments (essentially union of chains) give us:

THEOREM 15. Suppose $\mathfrak{M} \models T_\forall$. Then there is an $\mathfrak{M}_1$ such that $\mathfrak{M}_1$ is *T-e.c.*

and $\mathfrak{M} \subseteq \mathfrak{M}_1$. Moreover, $\mathfrak{M}_1$ can be chosen to have cardinal $\max(\text{card}(\mathfrak{M}), \text{card}(L))$.

Notation. E_T = class of T -e.c. structures.

I recommend SIMMONS [1972a] for the basic material on E_T . There is for example the following implicit definition of E_T :

E_T is the unique class $\mathcal{C}$ of models of $T_{\forall}$ such that

- (i) every model of $T_{\forall}$ is embeddable in a member of $\mathcal{C}$;
- (ii) if $\mathfrak{M}, \mathfrak{N} \in \mathcal{C}$ and $\mathfrak{M} \subseteq \mathfrak{N}$ then $\mathfrak{M} <_1 \mathfrak{N}$;
- (iii) if $\mathfrak{N} \in \mathcal{C}$ and $\mathfrak{M} <_1 \mathfrak{N}$ then $\mathfrak{M} \in \mathcal{C}$.

So the class E_T is mutually model consistent with the class of models of T , and E_T satisfies the conditions of Robinson's Test. Thus $\text{Th}(E_T)$ is a good candidate for a model companion of T . The snag is that E_T may not be an EC_{Δ} .

Now we can define a new companion operator.

DEFINITION. $T^{\circ} = \text{Th}(E_T)$.

THEOREM 16. $T \mapsto T^{\circ}$ is a companion operator.

This is a trivial verification.

COROLLARY. If T^* exists, then $T^* = T^{\circ}$.

But we can say more.

THEOREM 17 (EKLOF and SABBAGH [1971]). T has a model companion if and only if E_T is EC_{Δ} .

PROOF. ($\Leftarrow$) E_T satisfies conditions of Robinson's Test, so if it is elementary then $\text{Th}(E_T)$ is model complete.

($\Rightarrow$) If T^* exists, $T^* = T^{\circ}$, so T° is model complete. If $\mathfrak{M} \models T^{\circ}$, $\mathfrak{M} \subseteq \mathfrak{M}_1$ for some $\mathfrak{M}_1 \in E_T$. So $\mathfrak{M} < \mathfrak{M}_1$, since T° is model complete. By (iii) of the implicit definition, $\mathfrak{M} \in E_T$. $E_T = \text{Mod}(T^{\circ})$, so E_T is EC_{Δ} .

This theorem gives us a workable criterion for showing that certain theories have no model companion. Here is a typical application, which suggested a lot of later research.

Example (EKLOF and SABBAGH [1971]). T = group theory. Let $\mathfrak{M}_n$ ($n \in \omega$)

be in E_T . It is trivial that there exist in $\mathfrak{M}_n$ elements x_n, y_n of orders $n+1, n+2$ respectively. Let D be a non-principal ultrafilter on ω , and let $\mathfrak{M} = \prod \mathfrak{M}_n / D$. If E_T is EC_Δ , then $M \in E_T$. But this gives a contradiction, thus. Let $x = \prod x_n / D$, $y = \prod y_n / D$, with the obvious notation. By the Fundamental Theorem on ultraproducts, x and y have infinite order. So by a basic combinatorial result (HIGMAN, NEUMANN and NEUMANN [1949]) there exists a group extending $\mathfrak{M}$, with an element t such that $t^{-1}xt = y$. Since $\mathfrak{M} \in E_T$, there must be such an element t in $\mathfrak{M}$. But then $\{n \in \omega : x_n \text{ and } y_n \text{ are conjugate in } \mathfrak{M}_n\} \in D$. But this set is empty, since x_n and y_n have different orders.

Note. An almost identical argument works for skew fields (SABBAGH [1970]). Related arguments work for nilpotent groups (SARACINO [1974b]), solvable groups (SARACINO [1974a]), Lie algebras (MACINTYRE [1974b]), commutative rings (CHERLIN [1973]), modules over non-coherent rings (EKLOF and SABBAGH [1971]).

Thus for these classes we cannot easily understand the existentially closed structures.

3.4. The argument for Theorem 17 really shows that if T^* exists, then E_T is EC_Δ and $T^* = \text{Th}(E_T)$. So we can identify E_T for such classes as fields, and ordered fields, by the results of Section 2. In this light we see T^* as a *metamathematical* analogue of *algebraic closure*. Later, however, in the case of differential fields, we shall see that in analyzing the models of T^* we may not get too much help from thinking of the transparent example of algebraically closed fields. The prime model extension phenomena of Section 2 do not drop out from model completeness. It was at this point that Morley's analysis (MORLEY [1965]) of *algebraic* became relevant to algebra.

3.5. The forcing constructions

In 1969 there was an unexpected development. Since 1963, people had tried, with little success, to modify Cohen forcing (COHEN [1966]) into a general model theoretic construction. In Reyes' thesis (REYES [1967]) there is a Baire category approach linking forcing with homogeneous universal models. Reyes essentially obtained the notion of infinite forcing, which ROBINSON [1971] would develop in a more formal way in 1969–1970. But first Robinson invented finite forcing (BARWISE and ROBINSON [1970]), also known as model-theoretic forcing. The foundations of the subject are in Keisler's contribution to this book.

I want to say a little about forcing as a method of construction, and to explain the basic properties of the forcing companions.

T is given. There is a notion of forcing relative to T . The conditions are essentially finite fragments of diagrams of models of T . To construct a model by finite forcing one typically constructs larger and larger finite fragments of its diagram. The method is somehow like that involved in constructing recursively enumerable sets. If this remark is taken seriously, one can get applications by mixing combinatorial algebra and recursion theory (MACINTYRE [1972a]). One of the effects of Robinson's development was to bring together classical model theory and recursion theory (MACINTYRE [1972a]).

Once we have set up finite forcing relative to T , we define T^f , the finite forcing companion of T , by

$$T^f = \{\varphi \mid \emptyset \Vdash \neg \neg \varphi\}.$$

It is routine to prove that T^f is a consistent theory. The following theorem holds even for uncountable logics L . The proof is in BARWISE and ROBINSON [1970].

THEOREM 18. (a) $T \mapsto T^f$ is a companion operator.

(b) T^f is complete if and only if T has the Joint Embedding Property.

Then one gives (BARWISE and ROBINSON [1970]) a general definition of F_T , the class of (finite) generic models. In general, if $\mathfrak{M} \in F_T$, $\mathfrak{M} \models T^f$. But if L is uncountable, F_T may be empty (HENRARD [1971], SHELAH [1972a]).

The general facts are:

THEOREM 19. (a) If L is countable, $F_T \neq \emptyset$ and $T^f = \text{Th}(F_T)$;

(b) $F_T \subseteq E_T$;

(c) $\mathfrak{N} \in F_T$, $\mathfrak{M} <_1 \mathfrak{N}$ implies $\mathfrak{M} \in F_T$;

(d) $\mathfrak{M} \in F_T$ if and only if $\mathfrak{M}$ completes T^f , i.e. iff $\mathfrak{M} \subset \mathfrak{N} \models T^f$ implies $\mathfrak{M} < \mathfrak{N}$;

(e) T^* exists if and only if F_T is EC_Δ .

The proofs (BARWISE and ROBINSON [1970]) do not involve any complications.

We now have:

$$T^0 \subseteq T^e \subseteq T^f.$$

Each inclusion is proper when T is group theory (MACINTYRE [1972]).

Notes. (1) Later, ways were found of constructing T^i and F_T without forcing (SIMMONS [1973b], HENRARD [1973]). Also, one can implicitly define F_T along the lines of the definition for E_T (SIMMONS [1972b]).

(2) There is an important connection between the above forcing and the Omitting Types Theorem. The two methods are in some sense the same (KEISLER [1973], SIMMONS [1973a]). One should also look at SHELAH [1972].

3.6. Infinite forcing

This is a blunter instrument than finite forcing, as far as constructing models is concerned. But it has nice properties, which can be rapidly developed.

Again we fix T . This time we define a relation

$$\mathcal{M} \Vdash \varphi(\mathbf{m}) \quad (\mathcal{M} \text{ forces } \varphi)$$

where $\mathcal{M} \models T_\forall$, φ is an L-formula, and $\mathbf{m}$ is a tuple from $\mathcal{M}$.

The definition is the obvious one, with the all important recursion clause

$$\mathcal{M} \Vdash \neg \varphi \quad \text{iff} \quad \text{there is no } \mathcal{N} \text{ with } \mathcal{M} \subseteq \mathcal{N} \models T_\forall \text{ and } \mathcal{N} \models \varphi.$$

There is an obvious definition of generic model. $\mathcal{M}$ is generic if forcing and satisfaction coincide on $\mathcal{M}$. Let G_T be the class of generics, and let $T^s = \text{Th}(G_T)$.

One has the following implicit definition of G_T :

THEOREM 20 (ROBINSON [1971]). *G_T is the unique class $\mathcal{C}$ of models of $T_\forall$ such that*

- (i) *every model of $T_\forall$ is embeddable in a member of $\mathcal{C}$;*
- (ii) *if $\mathcal{M}, \mathcal{N} \in \mathcal{C}$ and $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{M} < \mathcal{N}$;*
- (iii) *if $\mathcal{N} \in \mathcal{C}$ and $\mathcal{M} < \mathcal{N}$, then $\mathcal{M} \in \mathcal{C}$.*

This again makes it clear that T^s is a candidate for T^* .

THEOREM 21. (a) $T \mapsto T^s$ is a companion operator;

(b) $G_T \subseteq E_T$;

(c) T^s is complete iff T has the Joint Embedding Property;

(d) T^* exists iff G_T is EC_Δ .

There is an interesting connection with homogeneous universal models. One sees that the latter are existentially closed in a very strong sense — certain infinite systems of equations and inequations may be allowed.

This leads to:

DEFINITION. Suppose $\mathcal{M} \models T_v$. $\mathcal{M}$ is *T-existentially universal* (*T-e.u.*) if whenever $\mathcal{M} \subseteq \mathcal{N} \models T_v$ and $\Sigma(v)$ is a set of basic formulas over $\mathcal{M}$, with finitely many free variables v , and $\text{card}(\Sigma) < \text{card}(\mathcal{M})$, then

$$\mathcal{N} \models \exists v \Sigma(v) \text{ implies } \mathcal{M} \models \exists v \Sigma(v).$$

Homogeneous universal models of T_v are clearly *T-e.u.*

The following nice theorem shows how to get G_T without forcing:

THEOREM 22 (FISHER [1970], WOOD [1972]). $\mathcal{M} \in G_T$ if and only if there is a $\mathcal{N}$ such that $\mathcal{N}$ is *T-e.u.* and $\mathcal{M} < \mathcal{N}$.

I recommend WOOD [1972] for an elegant account of the preceding, and for extensions to infinitary logic.

Notes. (1) MANEVITZ [1975] showed that G_T is not absolute for models of ZFC containing T . Both F_T and E_T are absolute.

(2) Suppose T is countable. Then (see MACINTYRE [1972b]) E_T and F_T are axiomatizable by single sentences of $L_{\omega_1\omega}$. G_T is axiomatizable by a set of sentences of $L_{\omega_1\omega}$ (WOOD [1972]), but not in general by a single sentence (MACINTYRE [1975a]).

3.7. Connecting T^f and T^s

We have now

$$T^0 \subseteq T^e \begin{matrix} \subseteq T^f \\ \subseteq T^s \end{matrix}$$

All inclusions are, in general, proper (MACINTYRE [1972]), and $T^f \cap T^s$ may be bigger than T^e . Note that $T^f \cap T^s$ is also a companion operator, but does not satisfy the Joint Embedding Condition that T^f and T^s do. Finally, $T^f \cup T^s$ can be inconsistent (MACINTYRE [1972a]).

3.8. In some unpublished work from 1971–1972, I looked at other notions of *T*-forcing and forcing companions (MACINTYRE [1972c]). One can force with recursive conditions, etc. I found this useful in group theory.

3.9. Connections between categoricity and model completeness

There are easy examples to show that a complete κ -categorical theory T need not be model complete. But there is a nice theorem of Lindström linking the two. Recall that a model complete theory T must be $\forall\exists$.

THEOREM 23 (LINDSTRÖM [1964]). Suppose T is complete $\forall\exists$ and κ -categorical, where $\kappa \geq \text{card}(L)$. Then T is model complete.

PROOF. Suppose not. Then by Löwenheim-Skolem there are models $\mathcal{M} \subset \mathcal{N}$ of T of power κ with $\mathcal{M} \not\prec_1 \mathcal{N}$. But $\mathcal{M}, \mathcal{N} \in E_T$, by categoricity. This is a contradiction. $\square$

3.10. Saracino found a slightly surprising connection between $\aleph_0$ -categoricity and model completeness.

THEOREM 24 (SARACINO [1973]). *Suppose L is countable, and T is complete $\aleph_0$ -categorical. Then T has a model companion T^* , and T^* is $\aleph_0$ -categorical.*

PROOF. We have to show that E_T is EC_Δ . Let $\psi(v)$ be a universal formula of L . Let $e(\psi)$ be the set of existential formulas $\varphi(v)$ such that T is a model of $\forall v (\varphi(v) \rightarrow \psi(v))$. This formula is *logically* equivalent to an $\forall$ -formula, so is a consequence of $T_\forall$. Now I quote the infinitary axioms for E_T , namely:

$$T_\forall \cup \left\{ \forall v \left(\psi(v) \leftrightarrow \bigwedge_{\varphi \in e(\psi)} \varphi(v) \right) \right\}$$

See SIMMONS [1972a]. But, given ψ , there are finitely many existential $\varphi_1, \dots, \varphi_n$ such that for any $\varphi, \varphi \in e(\psi)$, there is an $i, 1 \leq i \leq n$, such that $T \models \forall v (\varphi(v) \leftrightarrow \varphi_i(v))$, by the familiar characterization of $\aleph_0$ -categoricity due to Ryll-Nardzewski (see CHANG and KEISLER [1973]). But $T \models \forall v (\varphi \leftrightarrow \varphi_i)$ iff $T_{\forall\exists} \models \forall v (\varphi \leftrightarrow \varphi_i)$. So, axioms for E_T are

$$T_{\forall\exists} \cup \forall v (\psi(v) \leftrightarrow \varphi_1(v) \vee \dots \vee \varphi_n(v)).$$

So $T^* = T^c$. I have now to show that T^* is $\aleph_0$ -categorical. We have to show T^* has $< \omega$ n -types for each n . T^* is model-complete, so we have to show T^* has only finitely many inequivalent existential formulas. But T and T^* have the same consistent $\exists$ -formulas, and $T_{\forall\exists} \subseteq T^*$, so the result is obvious. $\square$

Note. I have used only the following property of T — that T has only finitely many existential n -formulas. It is not clear to me that this is equivalent to $\aleph_0$ -categoricity.

Example. T = dense linear order with end-points. T^* = dense linear order without end-points.

Example. Certain Boolean extensions of finite models. See Section 6.

It is reasonable in virtue of the theorems of Lindstrom and Saracino to hope that if T is $\aleph_1$ -categorical, then T has an $\aleph_1$ -categorical model companion. Unhappily, this hope was dashed:

(i) T may not have a model companion (BELEGRADEK and ZILBER [1974], SARACINO [1975]).

(ii) If T has a model companion T^* , T^* may not be $\aleph_0$ -categorical (BELEGRADEK and ZILBER [1974]).

One should observe however that if t is κ -stable and has a model companion then the model companion is κ -stable too.

3.11. Skolemization

I wish to point out a recent, and surprising, theoretical advance by WINKLER [1975]. He shows that for many natural T (e.g. algebraically closed fields) the “free Skolemization” of T has a model companion. His proof involves the concept of *algebraic boundedness* arising from the study of $\aleph_1$ -categoricity (BALDWIN and LACHLAN [1971]).

4. Applications: Differentially closed fields and prime model extensions

4.1. The aim of this short section is mainly philosophical. I will discuss an interaction between logic and algebra which has a different nature from the “positive” applications of Section 2 and the “negative” applications to come in Section 5.

In this example Robinson’s ideas have to be supplemented by ideas from stability theory (MORLEY [1965], SHELAH [1972b]), and then logic contributes to the development of a branch of algebra.

4.2. Ritt (see RITT [1966]) introduced the notion of differential field. This is naturally formalized in the language of field theory augmented by a function symbol for the derivation. See SACKS [1972]. SEIDENBERG [1956] found a criterion which tells when a system Σ over a differential field F has a solution in a (differential) extension of F . More precisely, he produced an algorithm which to a finite system $\Sigma(v, m)$ assigned a $\forall_1$ -condition $\Sigma'(m)$ such that

$$F \models \Sigma'(m) \quad \text{iff} \quad \text{for some extension } F_1 \text{ of } F, \quad F_1 \models \exists v \Sigma(v, m).$$

So Σ is unsolvable in all extensions of F if and only if $F \models \neg \Sigma'$. $\neg \Sigma'$ is equivalent to an existential formula.

In characteristic 0, Σ' can be chosen quantifier-free. In positive charac-

teristic, Seidenberg's analysis is much more complicated, and it takes a bit of work to reformulate his original statement in the way given above.

At any rate, the fact that Σ' can be chosen $\forall_i$ easily gives us axioms for E_T where T is the theory of differential fields of some specified characteristic. So:

THEOREM 25 (ROBINSON [1959] for $p = 0$; WOOD [1973] for $p \neq 0$). *The theory of differential fields of characteristic p has a model companion.*

(The model companion is denoted by DCF_p .) Note that the axioms for T^* in this case were not too memorable.

For $p = 0$, T^* has elimination of quantifiers, so:

THEOREM 26 (ROBINSON [1959]). *The theory of differential fields of characteristic 0 has a model completion.*

Theorem 26 fails in characteristic $p \neq 0$, because of failure of the amalgamation property. See WOOD [1973].

It turned out however that in characteristic $p \neq 0$ we may adjoin to our language a function symbol extracting p -th roots (and giving 0 when elements are not p -th powers), and then find a natural theory of differential fields with a model completion. We consider the theory of perfect differential fields of characteristic p . To get this we add to the theory of differential fields of characteristic p the axiom

$$\forall x (D(x) = 0 \text{ implies } \exists y (y^p = x)).$$

WOOD [1973] showed that this theory has a model completion. The p -th root symbol gives quantifier elimination, because it makes the axioms universal. In the language of differential fields, the model completion is just the earlier DCF_p . In the extended language, the model completion is also called DCF_p .

4.3. There were several unusual features to this example

Firstly, the axioms for the model completions were nowhere near as perspicuous as in the case of fields or ordered fields.

The second point was more perplexing. Think back to Section 2. In these examples one had not merely the operation of model completion, but also an operation of *closure* on structures. For example, a field K has an algebraic closure $\bar{K}$ which is *prime* over it in the following sense: Any embedding $K \rightarrow L$, where L is algebraically closed, can be decomposed as

$$K \rightarrow \tilde{K} \rightarrow L.$$

Moreover, any two such prime extensions of K are isomorphic over K .

Finally, the prime extension is *minimal*. That is, the embedding $K \rightarrow \tilde{K}$ cannot be properly factorized as $K \rightarrow L \rightarrow \tilde{K}$, where L is algebraically closed.

There are analogous facts for the various examples in Section 2, and these facts are certainly of much interest to a model theorist.

The natural question is:

Closure Problem. Are there always such facts associated with the model completion of a universal theory?

For example, is there a good notion of differential closure of a differential field?

No such notion was known classically. So here we have a case where the metamathematical closure is known, but no operation of closure on the relevant structures.

East coast model theory was not able to clarify this matter further. Progress was made by combining the eastern and the western methods. BLUM [1968] showed that the concepts of MORLEY [1965] enable one to obtain a differential closure in characteristic 0.

4.4. In the examples of Section 2, the closure of K is algebraic over K , in the classical field-theoretic sense. This is not so in the differential case, simply because there are differential equations whose solutions are transcendental over $\mathbb{Q}$.

MORLEY [1965] provided a beautiful notion of *algebraic* in a general setting. In the formulation of BLUM [1968] there are notions α -*algebraic* for each ordinal α . The case $\alpha = 0$ is the familiar classical notion for fields. Blum showed that we have to use n -*algebraic* for all $n < \omega$ to construct the differential closure.

Her main results are:

THEOREM 27 (a) *Without using Seidenberg's result, and using instead an analysis of simple extensions, one can find the model completion DCF_0 , and with a much nicer set of axioms.*

(b) DCF_0 is ω -stable, and so every differential field of characteristic 0 has a prime model extension to a model of DCF_0 .

(c) *Seidenberg's result can be derived from the model theoretic analysis.*

(It should be pointed out that there is a residue of Seidenberg's analysis in Blum's work, in the form of certain reduction procedures.)

So now we have the notion of a *differential closure*, in characteristic 0.

Later, WOOD [1974] carried out a corresponding analysis for perfect differential fields of characteristic p . The analogues of (a) and (c) hold; (b) has to be modified, since the theory of perfect differential fields is not ω -stable. Wood showed that nevertheless it has the related property that the isolated points are dense, and so by MORLEY [1965] one has the prime model extension property of (b). So one has also a differential closure in characteristic p .

The question of uniqueness of differential closure is trickier. Actually the differential closure is unique, but this needed an advance by SHELAH [1972b] in the general theory. Shelah showed that for ω -stable T the prime model extension is unique. Later, in SHELAH [1975], he showed that for stable T the prime model extension is unique *if it exists*. SHELAH [1974] showed that DCF_p is stable.

So, putting together the material of the preceding paragraphs we get:

THEOREM 28. *The differential closure is unique in all characteristics.*

Minimality. Unfortunately, the differential closure is not minimal, at least in characteristic 0. This was proved independently by KOLCHIN [1974] and SHELAH [1974]. One should consult SHELAH [1972b] for the Morley–Shelah theory underlying this.

The characteristic p case is unresolved.

Notes. (1) In SACKS [1972] there is a Nullstellensatz which follows from the basic model completeness result.

(2) Till now there is no application with the impact of those in Section 2.

5. Negative applications: Groups, skew fields, and number theories

5.1. The new methods of Section 3 give new constructions for existentially closed structures. The main direction of the new “applications” was to show that E_T is an extremely complicated class, for certain natural T . Further, one could provide counterexamples to existence of closures and/or minimal closures. A very comprehensive account of this development has been published in HIRSCHFELD and WHEELER [1975]. We begin with a brief summary of the method, and then pass to more concrete algebraic problems.

5.2. The non-model-theoretic background needed is:

- (a) T = group theory: Combinatorial group theory as in HIGMAN, NEUMANN and NEUMANN [1949];
- (b) T = theory of skew fields: Cohn's work in COHN [1971b].
- (c) T = a number theory: the basic theory of r.e. sets, some ideas going back to RABIN [1961], and the theorem of MATEJASEVIC [1970].

The fundamental fact established in all three cases is:

There is a uniform method assigning to each $\mathcal{M}$ in E_T an interpretation $P(\mathcal{M})$ such that

- (a) $P(\mathcal{M})$ is a substructure of 2-nd order arithmetic;
- (b) the interpretation persists under extension;
- (c) if $\mathcal{M}$ is T -existentially universal, $P(\mathcal{M})$ is the standard model of 2-nd order arithmetic.

We can readily conclude that 2-nd order arithmetic is Turing reducible to T^s . The converse is a general fact for arithmetical T such as the examples given at the beginning of this section. So:

THEOREM 29 (HIRSCHFELD and WHEELER [1975], MACINTYRE [1971]). *For the T given above, T^s is not an analytic set.*

Along the same lines one shows:

THEOREM 30. *For the T given above, T^f is Δ_1^1 but not arithmetic.*

COROLLARY. $T^f \neq T^s$.

The proofs of these fundamental results involve much coding and definability theory. One should consult HIRSCHFELD and WHEELER [1975].

5.2. Existentially closed groups

A shortcoming of the work reported in 5.1 is that it does not give results which are intelligible to an algebraist unfamiliar with recursion theory. In this subsection I will describe some natural algebraic results proved by forcing.

In this subsection, T is the theory of groups, formalized in the usual logic with $\cdot, ^{-1}, e$. Since T is a universal theory, the members of E_T are groups and are in fact precisely the non-trivial algebraically closed groups considered by W. R. Scott in the early 1950's (SCOTT [1951]). Scott obtained essentially a special case of Theorem 15.

Later, NEUMANN [1952] showed that e.c. groups are simple. Also, a trivial counting argument gives $2^{\aleph_0}$ isomorphism-types of countable e.c. groups.

But it emerged that we knew no invariants for e.c. groups, i.e. we could not see how to tell apart, informatively, two countable e.c. groups. Confirmation of the difficulty came with the beautiful theorem of NEUMANN [1973]:

THEOREM 31. *Any finitely generated group which can be presented with solvable word-problem is embeddable in all e.c. groups.*

This gave a focus to efforts using finite forcing. Neumann had used Higman's Embedding Theorem (HIGMAN [1961]), and this would soon be used in combination with finite forcing (MACINTYRE [1972a]). Also, Neumann's result raised the question: Which finitely generated groups are embeddable in all existentially closed groups?

This turned out to have a nice answer, and an easy demonstration using finite forcing.

THEOREM 32 (MACINTYRE [1972a]). *If a finitely generated group does not have solvable word-problem, then there is an e.c. group in which it is not embeddable.*

(This is an instance of a general theorem applying to skew fields, Lie algebras, etc.)

So, for the first time, one had a purely algebraic criterion for when a finitely generated group has solvable word-problem. (Later, BOONE and HIGMAN [1974] gave a quite different criterion.)

But the most important problem was to construct countable e.c. groups that genuinely "look different". An observation of MACINTYRE [1972a] and FISHER [unpublished] gives:

THEOREM 33. *Two countable e.c. groups are isomorphic if and only if they have the same isomorphism-types of finitely generated subgroups.*

This suggests that the following problem might have a positive answer:

Bers' Problem: Are any two e.c. groups elementarily equivalent?

It turned out (MACINTYRE [1972a]) that the answer is negative. T^e is not a complete theory. I constructed a $\forall_4$ sentence φ (to be explained below), which has clear algebraic meaning in members of E_T , such that φ holds in some members of E_T and fails in others. Later, BELEGRADEK [1974a] and MILLER [1974] obtained an $\forall_3$ -sentence. On general grounds it is known that T^e is complete for $\forall_2$ sentences.

The new phenomenon first observed here is the following: There are classes $\mathcal{C}$ of groups such that $\mathcal{C}$ is not EC_Δ , but $\mathcal{C} \cap E_T$ is of the form $\mathcal{C}_1 \cap E_T$, where $\mathcal{C}_1$ is EC (axiomatizable by a single sentence). In other words, there are concepts which are not first order for the class of all groups, but are first order relative to the class of e.c. groups.

A trivial example is:

$$\mathcal{C} = \text{class of simple groups.}$$

More complex examples are:

(1) $\mathcal{C}$ = class of groups which have a 2-generator subgroup into which all other 2-generator subgroups are embeddable (MACINTYRE [1972]).

(2) For any finitely presented group $\mathcal{H}$, the class $\mathcal{C}$ of groups in which $\mathcal{H}$ is embeddable (BELEGRADEK [1974], MILLER [1974]).

Both proofs use combinatorial group theory and coding devices.

Bers' Problem was solved by showing that the class $\mathcal{C}$ of Example 1 gives a non-trivial partition of E_T . To show this, I used Higman's universal finitely presented group (HIGMAN [1961]) and a finite forcing argument. This gives $\mathcal{C} \cap E_T \neq \emptyset$. To get $E_T \not\subseteq \mathcal{C}$, one observes that no existentially universal group is in $\mathcal{C}$, using a counting argument.

Let Max be the sentence describing $\mathcal{C} \cap E_T$. Max is $\forall_4$. Later (unpublished), using forcing with conditions recursively enumerable in a certain set, I showed that every countable member of E_T is embeddable in a member of $\mathcal{C}$. Also, BELEGRADEK [1974b], MACINTYRE [1971], MILLER [1974] and WHEELER [1972] independently proved that there are $2^{\aleph_0}$ elementary types of e.c. groups, and I proved that there are $2^{\aleph_0}$ elementary types satisfying Max. These results, being essentially codings of results about recursively enumerable sets, give much less *algebraic* information than the original solution to Bers' Problem.

Here are some other results proved by forcing (MACINTYRE [1972a]). (c) and (d) are in strong contrast to results of Sections 2 and 4.

(a) $G_T \cap F_T = \emptyset$;

(b) every countable e.c. group has a proper $L_{\infty, \omega}$ extension;

(c) every countable e.c. group contains a proper copy of itself (so there is no minimal member of E_T);

(d) there is no e.c. group embeddable in all others (so there is no prime model of E_T).

These results used in varying degrees material on the word-problem for groups. As might have been expected, such combinatorial techniques mix nicely with finite forcing.

Later results. BELEGRADEK [1974a, b] and MILLER [1974] obtained good

new results on the problem of when one can put one given group in as a subgroup of an e.c. group, and leave out another given one. Very recently ZIEGLER [1975] improved (b) to get extensions of each infinite cardinal, superseding MACINTYRE [1973b]. In particular, F_T has members of all infinite cardinalities.

5.3. Skew fields

The study of e.c. skew fields began in 1970, once COHN [1971b], in a brilliant advance, made available suitable analogues of the combinatorial techniques in group theory. SABBAGH [unpublished] quickly showed that there is no model companion for the theory of skew fields. Later work was done by BOFFA and VAN PRAAG [1972], MACINTYRE [1971] and WHEELER [1972].

For this subsection, let T be the theory of skew fields.

In MACINTYRE [1971] I showed that T^s is not analytic and T^f is not arithmetic. Also, there are $2^{\aleph_0}$ elementary types of members of E_T . The proofs used finite forcing, and did not have much explicit algebraic content, being codings of phenomena in recursion theory. Independently, WHEELER [1972] found much nicer proofs. We both did the analogue of (a) from 5.2, and Wheeler did (b) and (c). To get (d), I had first to prove (MACINTYRE [1973c]) the unsolvability of the word-problem for skew fields.

There are some major problems open. There is an analogue of Max (cf. 5.2) for skew fields, but it is unknown if there are members of E_T satisfying Max. The main problem is the absence of an embedding theorem of Higman type (cf. 5.2). To get such a theorem seems rather hard. Anyone interested should look at MACINTYRE [1975b]. So at present there is no natural way of telling e.c. skew fields apart. Another problem is to extend the final results of 5.2 to skew fields.

Nullstellensatz. It is rather disappointing that the structure of e.c. skew fields is so complex. For one might have hoped they would be a useful tool in ring theory, and a setting for some future non-commutative algebraic geometry.

What about a Nullstellensatz? Let K be a skew field, and let $K\langle x_1, \dots, x_n \rangle$ be the ring of polynomials over K in non-commuting variables $x_1, \dots, x_n$, not commuting with K . Suppose now K is e.c. and I is an ideal in $K\langle x_1, \dots, x_n \rangle$ with a zero in some extension skew field. Does I have a zero in K ?

It obviously does, if I is finitely generated. But WHEELER [1972], on the basis of the analogue of 5.2 (b), (c), gave a counterexample to the general case.

For *existentially universal* skew fields the Nullstellensatz does not fare quite so badly, and there is still some hope for an algebraic geometry.

5.4. Number theories

Let T be full number theory. In BARWISE and ROBINSON [1970], it is proved that $F_T = \{\mathbb{N}\}$, and in fact $\text{Mod}(T) \cap E_T = \{\mathbb{N}\}$. In ROBINSON [1973] he showed that one can define $\mathbb{N}$ in any member of E_T (cf. 5.2). His proof uses a technique pioneered by RABIN [1961], with simple sets used instead of creative sets.

Later the whole area was investigated systematically by GOLDREI, MACINTYRE and SIMMONS [1973] and HIRSCHFELD [1972]. See also HIRSCHFELD and WHEELER [1975]. The general flavor of results is that the situation is as chaotic as for groups and skew fields. The proofs use the same mixture of model theory and theory of recursively enumerable sets.

5.5. Other systems

There is reason to believe that Lie algebra, nilpotent groups of specified class, and solvable groups of specified class, will have E_T as complex as the above. See MACINTYRE [1974b] and SARACINO [1974a, 1974b], and MACINTYRE and SARACINO [1974].

For commutative rings, the situation is more obscure. There is no model-companion (CHERLIN [1973]), but no evidence of combinatorial complexity has been found (despite TAITSLIN [1974]).

6. Sheaves and model completeness

6.1. I want to end with a subject where there are positive results, connections with Section 2, and some unexplored research paths. The discussion will be brief, since I wish mainly to communicate some formal ideas.

The starting point is a theorem of CARSON [1973] and LIPSHITZ and SARACINO [1973]. They proved that the theory of commutative rings with 1 and *no non-zero nilpotent elements* has a model companion. (Contrast this with CHERLIN [1972], cited in 5.) In fact, they gave nice axioms for existentially closed commutative regular rings with 1. It is easy to see the mutual model-consistency of the theory of commutative rings with 1 and no non-zero nilpotents, and the theory of commutative regular rings with 1. It is more convenient in what follows to work with T , the theory of commutative regular rings with 1.

In order to reach a general viewpoint, Carson's sheaf-theoretic analysis

seems to me more natural. By general representation theory (PIERCE [1967]) any model of T is isomorphic to the ring of global sections of a sheaf $\mathcal{S}$, of fields, over a *Boolean* space X . With the Boolean space one has its dual algebra B , and in this case B is the algebra of idempotents of the original ring. Now it emerged from the analysis of the above authors that the members of E_T are precisely those models of T where B is *atomless*, and the stalks of the sheaf are *algebraically closed fields*.

But now the pattern is clear. To get the model companion of T we do two things:

- (i) Take the model companion of the theory of Boolean algebras (cf. 3.2, Example 4);
- (ii) take the model companion of the theory of the stalks.

Then the members of E_T are sections of sheaves over spaces X , where X is Boolean with atomless dual, and the stalks are models of the model companion of the theory of the stalks of the original class of sheaves.

MACINTYRE [1973a] and WEISSPFENNING [1973], on the basis of this formal observation, put the Carson–Lipshitz–Saracino result into a general setting. Here is a specimen result:

THEOREM 34 (MACINTYRE [1973a]). *Let T_1 be a theory of fields. Suppose T_1 is model-complete. Let T be the theory of rings of sections of sheaves $\mathcal{S}$, with stalks models of T_1 , and over a Boolean space without isolated points. Then T is model complete.*

When T_1 is the theory of fields, we get the Carson–Lipshitz–Saracino theorem. VAN DEN DRIESS [1975], MACINTYRE [1973a] and WEISSPFENNING [1973] looked at what happens when T_1 is the theory of real closed fields. It turns out that this gives the existence of a model-companion for a class of lattice-ordered rings, the so-called regular f -rings (see BURKHOFF [1967]).

The general principle is that any of the model completeness results of Section 2 will transform to an analogous result about regular rings. For example, VAN DEN DRIESS [1975] and WEISSPFENNING [1973] have results on differential rings. The p -adic case has not been closely studied.

6.2. The results above are not in general as strong as those of Section 2. The problem is that we do not in general have a prime model extension to a member of E_T . See SARACINO and WEISSPFENNING [1973]. For T = theory of regular rings, LIPSHITZ [1974a] has greatly clarified the question of the existence of prime model extensions.

In the real regular case (regular f -rings), there is a unique prime model

extension. See LIPSHITZ [1974b] and VAN DEN DRIESS [1975]. From this, Van den Driess obtained an analogue of the solution of Hilbert's 17-th Problem for real regular rings. I believe Robinson would have admired this result.

Notes. (1) This material connects with $\aleph_0$ -categoricity. By results of WEGŁOZ and WASKIEWICZ [1968], a Boolean extension of an $\aleph_0$ -categorical structure by an atomless Boolean algebra is $\aleph_0$ -categorical. So by SARACINO [1973], its theory has a model companion. On the other hand, a Boolean extension *is* the structure of sections of a sheaf over a Boolean space. Is the model companion the theory of some natural Boolean extension?

(2) In my version of Theorem 34 I used Comer's results (COMER [1974]) on Feferman–Vaught theorems for sheaves. Later Comer using the formal principle of 6.1 obtained model completeness results for polyadic algebras (COMER [1973]).

(3) It seems to me that the results of this section should be interpreted topoi-theoretically, i.e. by doing model theory inside a category of sheaves. The intuition is that the sheaf associated with an e.c. regular ring is an algebraically closed field in the sense of a category of sheaves. Work is under way on this and related matters (JOYAL [1975], LOULLIS [1976]).

Acknowledgment

I wish to thank Carol Wood who kindly read the manuscript and made many valuable criticisms.

References

- ADLER, A., and K. KIEFE
 [1976] Pseudofinite fields, procyclic fields and model-completion, *Pacific J. Math.*, **62**, 305–310
- ARTIN, E. and O. SCHREIER
 [1926] Algebraische Konstruktion reeller Körper, *Hamb. Abh.*, **5**, 85–99.
- ARTIN, E.
 [1927] Über die Zerlegung definiter Funktionen in Quadrate, *Hamb. Abh.*, **5**, 100–115.
- AX, J.
 [1968] The elementary theory of finite nelds, *Ann. of Math.*, **88**, 239–271
- AX, J. and S. KOCHEN
 [1965a] Diophantine problems over local fields I, *Am. J. Math.*, **87**, 605–630.
 [1965b] Diophantine problems over local fields II: A complete set of axioms for p -adic number theory, *Am. J. Math.*, **87**, 631–648.
 [1966] Diophantine problems over local fields III: Decidable fields, *Ann. of Math.*, **83**, 437–456.

- BACSICH, P.D. and D. ROWLAND-HUGHES
 [1974] Syntactic characterisations of amalgamation, convexity and related properties, *J. Symbolic Logic*, **39**, 433–451.
- BALDWIN, J.T. and A. H. LACHLAN
 [1971] On strongly minimal sets, *J. Symbolic Logic*, **36**, 79–96.
- BARWISE, J. and A. ROBINSON
 [1970] Completing theories by forcing, *Ann. Math. Logic*, **2**, 119–142.
- BELEGRADEK, O.B.
 [1974a] On algebraically closed groups, *Algebra i Logika*, **13**, 239–255 (Russian).
 [1974b] Personal communication, to appear.
- BELEGRADEK, O.B. and B.I. ZILBER
 [1974] The model companion of an $\aleph_1$ -categorical theory, Third All-Union Conference on Mathematical Logic, Institut Matematiki CO AH CCCP, Novosibirsk, 10 (Russian).
- BELL, J.L. and A.B. SLOMSON
 [1969] *Models and Ultraproducts* (North-Holland, Amsterdam).
- BURKHOFF, G.
 [1967] *Lattice Theory* (Am. Math. Soc., Providence, RI).
- BLUM, L.
 [1968] *Generalized Algebraic Theories*, Thesis, M.I.T. Press, Cambridge, MA.
- BOFFA, M. and P. VAN PRAAG
 [1972] Sur les corps generiques, *C.R. Acad. Sci. Paris Ser. A*, **274**, 1325–1327.
- BOONE, W. and G. HIGMAN
 [1974] An algebraic characterization of groups with soluble word problem, *J. Austral. Math. Soc.*, **18**, 41–53.
- CARSON, A.B.
 [1973] The model completion of the theory of commutative regular rings, *J. Algebra*, **27**, 136–146.
- CHANG, C.C. and H.J. KEISLER
 [1973] *Model Theory* (North-Holland, Amsterdam).
- CHERLIN, G.
 [1973] Algebraically closed commutative rings, *J. Symbolic Logic*, **38**, 493–499.
- COHEN, P.J.
 [1966] *Set Theory and the Continuum Hypothesis* (Benjamin, New York).
 [1969] Decision procedures for real and p -adic fields, *Comm. Pure Appl. Math.*, **22**, 131–151.
- COHN, P.M.
 [1971a] *Free Rings and Their Relations* (Academic Press, London).
 [1971b] The embedding of firs in skew fields, *Proc. London Math. Soc.*, **23**, 193–213.
- COMER, S.D.
 [1973] Complete and model-complete theories of polyadic algebras, Preprint. Vanderbilt University, Nashville, TN.
 [1974] Elementary properties of structures of sections, *Bol. Soc. Mat. Mexicana*, **19**, 78–85.
- COVEN, C.
 [1971] Forcing in infinitary languages Thesis. Yale University, New Haven, CT, Appendix.
- EKLOF, P. and G. SABBAGH
 [1971] Model completions and modules, *Ann. Math. Logic*, **2**, 251–295.
- ERSOV, YU. L.
 [1965] On the elementary theory of maximal normed fields, *Dokl. Akad. Nauk. SSSR*, **165**. [English translation in *Sov. Math Dokl.*, 1390–1393.]

- [1967] Fields with a solvable theory, *Dokl. Akad. Nauk SSSR*, **174**. [English translation in *Sov. Math. Dokl.*, 575–576.]
- FISHER, E.
 [1970] Homogeneous-universal models revisited, Yale notes, unpublished.
- FRIED, M. and G. SACERDOTE
 [1975] A primitive recursive procedure for solving diophantine problems over all residue class fields of a number field, and all finite fields. Preprint, University of California at Irvine.
- GAIFMAN, H.
 [1967] Uniform extension operators for models and their applications, in: *Sets, Models and Recursion Theory*, edited by J.N. Crossley (North-Holland, Amsterdam) pp. 122–155.
- GOLDREI, D.C., A. MACINTYRE and H. SIMMONS
 [1973] The forcing companions of number theories, *Israel J. Math.*, **14**, 317–337.
- GREENBERG, M.
 [1969] *Lectures on Forms in Many Variables* (Benjamin, New York).
- HENRARD, P.
 [1971] Une theorie sans modèle generique, *C.R. Acad. Sci. Paris Sér. A*, **272**, 293–294.
 [1973] Le “forcing-compagnon” sans “forcing”, *C.R. Acad. Sci. Paris Ser. A*, **276**, 821–822.
- HIGMAN, G., B.H. NEUMANN and H. NEUMANN
 [1949] Embedding theorems for groups, *J. London Math. Soc.*, **24**, 247–254.
- HIGMAN, G.
 [1961] Subgroups of finitely presented groups, *Proc. Roy. Soc. London Ser. A*, **262**, 455–475.
- HIRSCHFELD, J.
 [1972] Existentially complete and generic structures in arithmetic, Thesis, Yale University, New Haven, CT.
- HIRSCHFELD, J. and W.H. WHEELER
 [1975] *Forcing, Arithmetic, and Division Rings*, Lecture Notes in Mathematics, Vol. 454 (Springer, Berlin).
- JACOBSON, N.
 [1964] *Lectures in Abstract Algebra III* (Van Nostrand, New York).
 [1974] *Basic Algebra I* (Freeman, San Francisco, CA).
- JARDEN, M. and U. KIEHNE
 [1975] The elementary theory of algebraic fields of finite corank, *Invent. Math.*, **30**, 275–294.
- JENSEN, R.B.
 [1972] The fine structure of the constructible hierarchy, *Ann. Math. Logic*, **4**, 229–308.
- JONSSON, B.
 [1965] Extensions of relational structures, in: *The Theory of Models*, edited by J.W. Addison, L. Henkin and A. Tarski (North-Holland, Amsterdam) pp. 146–157.
- JOYAL, A.
 [1975] Structures generiques dans les topos et ailleurs. Contributed paper (abstract), Siecil, Clermont-Ferrand, 1975.
- KAISER, K.
 [1969] Über eine verallgemeinerung der Robinsonschen Modellvollständigkeit, *Z. Math. Logik Grundlagen Math.*, **15**, 37–48.
- KAPLANSKY, I.
 [1942] Maximal fields with valuation I, *Duke Math. J.*, **9**, 303–321.
- KEISLER, H.J.
 [1973] Forcing and the omitting types theorem, in: *Studies in Model Theory*, edited by M. Morley (Math. Assoc. Am., Buffalo, NY) pp. 96–133.

KOCHEN, S.

[1961] Ultraproducts in the theory of models, *Ann. of Math.*, **74**, 221–261.

[1969] Integer valued rational functions over the p -adic numbers: a p -adic analogue of the theory of real fields, in: *Proceedings of Symposia in Pure Mathematics, XII, Number Theory*, edited by W.J. Leveque and E.G. Strauss (Am. Math. Soc., Providence, RI) pp. 57–73.

KOLCHIN, E.

[1974] Constrained extensions of differential fields, *Advances in Math.*, **12**, 141–170.

LANG, S.

[1952] On quasi algebraic closure, *Ann. of Math.*, **55**, 373–390.

[1958] *Algebraic Geometry* (Addison-Wesley, New York).

LINDSTROM, P.

[1964] On model-completeness, *Theoria*, **30**, 183–196.

LIPSHITZ, L.

[1974a] Prime model extensions for commutative regular rings, *Trans. Am. Math. Soc.*, to appear.

[1974b] The real closure of a commutative regular f -ring. Preprint, Purdue University, Lafayette, IN.

LIPSHITZ, L. and D. SARACINO

[1973] The model companion of the theory of commutative rings without nilpotent elements, *Proc. Am. Math. Soc.*, **37**, 381–387.

LOULLIS, G.

[1976] Some aspects of the model theory on a topos. Thesis, Yale University, New Haven, CT, to appear.

MACINTYRE, A.

[1971] On algebraically closed division rings, unpublished.

[1972a] On algebraically closed groups, *Ann. of Math.*, **96**, 53–97.

[1972b] Omitting quantifier-free types in generic structures, *J. Symbolic Logic*, **37**, 512–520.

[1972c] Lecture notes on forcing in model theory, Berlin, unpublished.

[1973a] Model completeness for sheaves of structures, *Fund. Math.*, **LXXXI**, 73–89.

[1973b] The word problem for division rings, *J. Symbolic Logic*, **38**, 428–436.

[1973c] Martin's Axiom applied to existentially closed groups, *Math. Scand.*, **32**, 46–56.

[1974a] On definable sets of p -adic numbers, *J. Symbolic Logic*, to appear.

[1974b] Existentially closed Lie algebras, Abstract 74T-E38, *Notices Am. Math. Soc.*, **21**, A-379.

[1975a] A note on axioms for infinite-generic structures, *J. London Math. Soc.*, **9**, 581–584.

[1975b] Combinatorial problems for skew fields, Yale University, New Haven, CT, preprint.

MACINTYRE, A. and D. SARACINO

[1974] On existentially closed nilpotent Lie algebras, Abstract 74T-E37, *Notices Am. Math. Soc.*, **21**, A-379.

MAKOWSKY, J.A.

[1973] On continuous quantifiers, Abstract 73T-E84, *Notices Am. Math. Soc.*, **20**, A-502.

MANEVITZ, L.

[1975] Model theoretic forcing and absoluteness, Thesis, Yale University, New Haven, CT.

MATEJASEVIC, JU. V.

[1970] Enumerable sets are diophantine, *Sov. Math. Dokl.*, **11**, 354–358.

McKENNA, K.

[1975] Hilbert's 17-th Problem revisited, Yale University, New Haven, CT, preprint.

MILLER, C.W. III,

[1974] On algebraically closed groups, Princeton University, Princeton, NJ, preprint.

MORLEY, M.

- [1965] Categoricity in power, *Trans. Am. Math. Soc.*, **114**, 514–538.

NEUMANN, B.H.

- [1952] A note on algebraically closed groups, *J. London Math. Soc.*, **27**, 247–249.
 [1973] The isomorphism problem for algebraically closed groups, in: *Word Problems*, edited by B.B. Boone, F.B. Cannonito and R.C. Lyndon (North-Holland, Amsterdam) pp. 553–562.

PIERCE, R.S.

- [1967] Modules over commutative regular rings, *Mem. Am. Math. Soc.*, **70**.

PRESBURGER, M.

- [1930] Ueber die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchen die Addition als einzige Operation hervortritt, in: *Comptes Rendus du I Congrès de Mathématiciens des Pays Slaves* (Warsaw) pp. 92–101.

RABIN, M.O.

- [1961] Non-standard models and the independence of the induction axiom, in: *Essays on the Foundations of Mathematics* (Magnes Press, Jerusalem) pp. 287–299.

REYES, G.E.

- [1967] Typical and generic in a Baire space for relations, Thesis, Berkeley.

RITT, J.

- [1966] *Differential Algebra* (Dover, New York).

ROBINSON, A.

- [1951] *On the Metamathematics of Algebra* (North-Holland, Amsterdam).
 [1955] On ordered fields and definite functions, *Math. Ann.*, **130**, 257–271.
 [1956] *Complete Theories* (North-Holland, Amsterdam).
 [1959a] On the concept of a differentially closed field, *Bull. Research Council, Israel*, (F), **8F**, 113–128.
 [1959b] Solution of a problem of Tarski, *Fund. Math.*, **47**, 179–204.
 [1963] *Introduction to Model Theory* (North-Holland, Amsterdam).
 [1971] Infinite forcing in model theory, in: *Proceedings of the Second Scandinavian Logic Symposium*, edited by J.E. Fenstad (North-Holland, Amsterdam) pp. 317–340.
 [1973] Non standard arithmetic and generic arithmetic, in: *Logic, Methodology and Philosophy of Science IV*, edited by P. Suppes et al. (North-Holland, Amsterdam) pp. 137–154.

SABBAGH, G.

- [1970] Personal communication.

SACKS, G.

- [1972] *Saturated Model Theory* (Benjamin, New York).
 [1973] The differential closure of a differential field, *Bull. Am. Math. Soc.*, **78**, 629–633.

SARACINO, D.

- [1973] Model companions for $\aleph_0$ -categorical theories, *Proc. Am. Math. Soc.*, **39**, 591–598.
 [1974a] Wreath products and existentially complete solvable groups, *Trans. Am. Math. Soc.*, **197**, 327–339.
 [1974b] On existentially complete nilpotent groups, Abstract 74T-E36, *Notices Am. Math. Soc.*, **21**, A-379.
 [1973] A counterexample in the theory of model companions, Yale University, New Haven, CT, preprint.

SARACINO, D. and V. WEISSPENNING

- [1973] Commutative regular rings without prime model extensions, Yale University, New Haven, CT, preprint.

SCOTT, D

- [1969] Completing ordered fields, in: *Applications of Model Theory to Algebra, Analysis,*

and Probability, edited by W.A.J. Luxemburg (Holt, Rinehart and Winston, New York) pp. 274–278.

SCOTT, W.R.

[1951] Algebraically closed groups, *Proc. Am. Math. Soc.*, **2**, 118–121.

SEIDENBERG, A.

[1956] An elimination theory for differential algebra, *Univ. of California Math. Publications*, **3**, 31–65.

SHELAH, S.

[1971] Every two elementarily equivalent models have isomorphic ultrapowers, *Israel J. Math.*, **10**, 224–233.

[1972a] A note on model complete models and generic models, *Proc. Am. Math. Soc.*, **34**, 509–514.

[1972b] Uniqueness and characterization of prime models over sets for totally transcendental first-order theories, *J. Symbolic Logic*, **37**, 107–113.

[1973] Differentially closed fields, *Israel J. Math.*, **16**, 314–328.

[1975] Uniqueness of prime models, with an application to differential fields. Abstract 74T-E17, *Notices Am. Math. Soc.*, **21**, A-318.

SHOENFIELD, J.R.

[1971] A theorem on quantifier elimination, *Symposia Math.*, **5**, 173–176.

SIMMONS, H.

[1972a] Existentially closed structures, *J. Symbolic Logic*, **37**, 293–310.

[1972b] A possible characterization of generic structures, *Math. Scand.*, **31**, 257–261.

[1973a] An omitting types theorem with an application to the construction of generic structures, *Math. Scand.*, **33**, 46–53.

[1973b] Une construction du forcing-compagnon d'une theorie, *C.R. Acad. Sci. Paris Sér. A*, **277**, 563–566.

[1975] *Companion Theories (Forcing in Model Theory)* (Vander, Louvain).

TAITSLIN, M.

[1974] Existentially closed commutative rings, Third All-Union Conference on Mathematical Logic, Institue Matematiki CO AH CCCP, Novosibirsk, 213–215 (Russian).

TARSKI, A.

[1951] *A Decision Method for Elementary Algebra and Geometry* (Univ. of California Press, Berkeley, 2nd. revised ed.).

TARSKI, A. and R.L. VAUGHT

[1957] Arithmetical extensions of relational systems, *Compositio Math.*, **13**, 81–102.

TERJANIAN, G.

[1966] Un contre-exemple a une conjecture d'Artin, *C.R. Acad. Sci. Paris Ser. A*, **262**, 612.

VAN DEN DRIESS, L.

[1975] Artin-Schreier theory for commutative regular rings, University of Utrecht, Utrecht, preprint.

VAUGHT, R.L.

[1965] The Löwenheim-Skolem Theorem, in: *Logic, Methodology and Philosophy of Science*, edited by Y. Bar-Hillel (North-Holland, Amsterdam, 2nd repr. 1972) pp. 81–89.

WASKIEWICZ, J. and B. WEGŁOZ

[1968] Some models of theories of reduced powers, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, **16**, 683–685.

WEISSPFENNING, V.

[1971] On the elementary theory of Hensel fields, Thesis, University of Heidelberg, Heidelberg.

- [1973] Model completeness and elimination of quantifiers for subdirect products, *J. Algebra*, to appear.
- WHEELER, W.H.
- [1972] Algebraically closed division rings, forcing, and the analytic hierarchy, Thesis, Yale University, New Haven, CT.
- WINKLER, P.
- [1975] Assignment of Skolem functions for model complete theories, Thesis, Yale University, New Haven, CT.
- WOOD, C.
- [1972] Forcing for infinitary languages, *Z. Math. Logik Grundlagen Math.*, **18**, 385–402.
- [1973] The model theory of differential fields of characteristic $p \neq 0$, *Proc. Am. Math. Soc.*, **40**, 577–584.
- [1974] Prime model extensions for differential fields of characteristic $p \neq 0$, *J. Symbolic Logic*, **39**, 469–477.
- ZIEGLER, M.
- [1972] Die elementäre Theorie des Henselchen Körper, Thesis, University of Köln, Cologne.
- [1975] Personal communication.

Homogenous Sets

MICHAEL MORLEY

Contents

1. Introduction	182
2. Partition theorems and the E.-M. theorem	182
3. Skolem functions and elementary submodels	185
4. ω -logic	187
5. Types and Ehrenfeucht–Mostowski models	189
6. Partition theorems for large cardinals and the constructible universe	193
References	196

1. Introduction

A free group on a set X of generators has the property that every one-one map of X into itself induces a monomorphism of the group into itself. Further, if the one-one map of X is surjective, the induced monomorphism is actually an automorphism.

To what extent can models with similar properties be constructed for general theories? (By theory we usually, but not always, mean a theory in the language of the first order calculus.) More precisely, for a given set X , is there a model $\mathfrak{A}$ of T such that every one-one map of X into itself induces a monomorphism of $\mathfrak{A}$? Obviously, if T involves a linear ordering, non-order preserving permutations of X can not be extended to monomorphisms of $\mathfrak{A}$. Rather surprisingly, the following theorem states that linear orderings are the only exception to the rule.

1.1. THEOREM (Ehrenfeucht–Mostowski). *Let T be a countable theory of the predicate calculus which has an infinite model and let $\langle X, < \rangle$ be an infinite linearly ordered set. There is a model $\mathfrak{A}$ of T with $X \subseteq A$ such that every order preserving map of X into itself induces a monomorphism of $\mathfrak{A}$ into itself and every order preserving onto map of X induces an automorphism of $\mathfrak{A}$.*

Models with interesting properties can be constructed by varying the order type of $\langle X, < \rangle$. Part of the sequel will be devoted to showing to what extent $\mathfrak{A}$ is determined by the order type of $\langle X, < \rangle$.

Section 2 is devoted to proving a weak form of the Ehrenfeucht–Mostowski theorem. Section 3 discusses how to generate submodels and strengthens the results of Section 2. Section 4 discusses extensions of the Ehrenfeucht–Mostowski theorem to non-elementary languages. Section 5 gives an application of the Ehrenfeucht–Mostowski theorem to group theory and discusses theories whose models contain relatively large homogenous sets. Section 6 considers some implications of the existence of homogenous sets of order type ω_1 in models of set theory.

2. Partition theorems and the E.–M. theorem

First, the introduction of some notations and definitions. The notation $X^{(n)}$ signifies the set

$$X^{(n)} = \{y: y \subseteq X \text{ and } |y| = n\}.$$

As we shall assume the axiom of choice throughout, we may as well consider the set X to be linearly ordered. The set $X^{(n)}$ is the set of n -tuples $\{(x_0, \dots, x_{n-1}); x_i \in X, x_0 < x_1 < \dots < x_{n-1}\}$. We shall refer to $X^{(n)}$ as the set of properly ordered n -tuples of X .

The ordinal γ is the set of ordinals $< \gamma$. As usual, the least cardinal $> \kappa$ is written κ^+ . For each ordinal α , $2(\kappa, \alpha)$ is defined by induction:

$$2(\kappa, 0) = \kappa$$

$$2(\kappa, \alpha) = \sup\{2^{2(\kappa, \beta)}; \beta < \alpha, \alpha > 0\}.$$

In particular, define

$$\mathfrak{J}_\alpha = 2(\omega, \alpha).$$

The generalized continuum hypothesis in this notation is $\kappa_\alpha = \mathfrak{J}_\alpha$ for all α .

Assume a partition P of $X^{(n)}$ into μ disjoint classes. A set $Y \subset X$ is homogenous for P if $Y^{(n)}$ is included in one partition class. If for any set X of power κ and any partition P of $X^{(n)}$ into μ disjoint classes, X contains a set Y homogenous for P of power λ , we write

$$\kappa \rightarrow (\lambda)_\mu^n.$$

Proofs for the following theorems about the cardinality of homogenous sets are given in Chapter B.3 on combinatorics.

2.1. THEOREM (Ramsey's Theorem). *If m is finite, then*

$$\omega \rightarrow (\omega)_m^n.$$

2.2. THEOREM (Erdős-Rado). *For any infinite cardinal κ ,*

$$(2(\kappa, n))^+ \rightarrow (\kappa^+)_\kappa^{n+1}.$$

2.3. THEOREM (Erdős). *There is no cardinal κ such that*

$$\kappa \rightarrow (\omega)_2^\omega$$

i.e. infinite homogenous sets do not exist for arbitrary partitions of the set $X^{(\omega)}$ of denumerable subsets of X .

2.4. THEOREM (Ehrenfeucht-Mostowski). *Let T be a countable theory in a language L of the predicate calculus which has an infinite model and let $\langle X, < \rangle$ be an infinite linearly ordered set. The theory T has a model $\mathfrak{A}$, $X \subseteq \mathfrak{A}$, with the property that for all n all properly ordered n -tuples $\langle x_0, \dots, x_{n-1} \rangle$ of X satisfy the same set of formulas $\varphi(v_0, \dots, v_{n-1})$ of L .*

Remarks. The set X is said to be homogenous for the model $\mathfrak{A}$. The set Φ of formulas satisfied by the properly ordered tuples of X is called an Ehrenfeucht–Mostowski (E.–M.) set. From the Compactness Theorem, it follows that for any E.–M. set Φ and linear ordering $\langle Y, < \rangle$, there is a model containing $\langle Y, < \rangle$ as a homogenous subset whose properly ordered tuples satisfy the formulas of Φ .

PROOF. Let $\mathfrak{B}$ be an infinite model of T and $\varphi_0, \varphi_1, \dots$ an enumeration of the formulas of L . Impose a linear ordering $<$ on B . (In general, this ordering is unrelated to the relations of $\mathfrak{B}$.) Suppose φ_0 has free variables $v_0, \dots, v_n$. The formula φ_0 determines a partition of $B^{(n+1)}$ into two classes depending on whether the properly ordered $n+1$ -tuple $\langle b_0, \dots, b_n \rangle$ satisfies φ_0 or not. By Theorem 2.2, there is an infinite $B_0 \subset B$ homogenous for this partition. Let φ_1 have free variables $v_0, \dots, v_k$. Then φ_1 determines a partition $B_0^{(k+1)}$ into two classes with an infinite homogenous subset $B_1 \subset B_0$. Continuing in this fashion, we construct a nested sequence $\{B_i: i \in \omega, B_{i+1} \subset B_i\}$ of infinite sets B_i . Enlarge L by adding a new constant x for each $x \in X$ and enlarge T by adding for each formula $\varphi_i \equiv \varphi_i(v_0, \dots, v_k)$ and each $x_0 < \dots < x_k$ of $X^{(k+1)}$ the sentence $\varphi_i(x_0, \dots, x_k)$ or $\neg \varphi_i(x_0, \dots, x_k)$ depending on whether the properly ordered $k+1$ -tuples of B_i satisfy φ or $\neg \varphi$. The enlarged theory is finitely consistent and so has a model $\mathfrak{A}$ satisfying the conclusion of the theorem, by the Compactness Theorem. $\square$

2.5. COROLLARY. *If $\varphi(v)$ is satisfied by an infinite set of elements in some model of T , then it is consistent to add the condition that the elements of $\langle X, < \rangle$ satisfy $\varphi(v)$ in the model $\mathfrak{A}$ of Theorem 2.4. If $\varphi(v_0, v_1)$ linearly orders an infinite set in a model of T , then in $\mathfrak{A}$ the ordering $<$ of X may be defined by φ .*

2.6. DEFINITION. A *subsystem* of a relation structure $\mathfrak{A}$ is any subset of A which is closed under the functions defined in $\mathfrak{A}$. A subsystem generated by a subset X of A is the smallest subsystem of $\mathfrak{A}$ containing X .

Thus, an element of a subsystem of $\mathfrak{A}$ generated by X is represented by a term $t(x_0, \dots, x_n)$ where $x_i \in X$ and t is built up from the functions of $\mathfrak{A}$.

Consider any order preserving map f of the set X homogeneous for the model $\mathfrak{A}$. The map f can be extended to the subsystem generated by X by defining

$$f(t(x_0, \dots, x_n)) = t(fx_0, \dots, fx_n).$$

It follows immediately from Theorem 2.4 that f induces a monomorphism of the subsystem into itself and that if f is actually onto, the monomorphism is an automorphism of the subsystem. Thus, if we can arrange that the subsystem of $\mathfrak{A}$ generated by X is actually a model of T , we will have accomplished the goal undertaken in Section 1. This feat constitutes the next section.

3. Skolem functions and elementary submodels

Let L be a language of the predicate calculus. Corresponding to each formula $\varphi(v_0, \dots, v_n)$ of L , introduce an n -ary function symbol f_φ (the Skolem function) to form a new language L^* . If $n = 0$, the Skolem function f_φ is a constant c_φ . The languages L_n^* and L^* are defined inductively:

$$L_0^* = L, \quad L_{n+1}^* = (L_n^*)',$$

$$L^* = \bigcup_{n \in \omega} L_n^*.$$

3.1. DEFINITION. The defining sentence of the *Skolem function* f_φ is the L^* sentence

$$\forall v_0 \cdots \forall v_{n-1} [\exists v_n \varphi(v_0, \dots, v_n) \rightarrow \varphi(v_0, \dots, v_{n-1}, f_\varphi(v_0, \dots, v_{n-1}))].$$

3.2. DEFINITION. A relation structure $\mathfrak{A}$ of the language L is a *Skolem model* if every defining sentence of L^* is valid in $\mathfrak{A}$. If T is a theory in L its Skolem closure is $T^* = T \cup \{\text{defining sentences of } L^*\}$.

3.3. DEFINITION. The terms of the language L^* are called *Skolem terms*.

Under the assumption of the axiom of choice, every relation structure $\mathfrak{A}$ of the language L can be expanded to a Skolem model $\mathfrak{A}^*$ with the same universe as $\mathfrak{A}$ such that for all formulas φ of L , $\mathfrak{A} \models \varphi(a_0, \dots, a_n)$, $a_i \in A$ if and only if $\mathfrak{A}^* \models \varphi(a_0, \dots, a_n)$.

3.4. DEFINITION. An *elementary submodel* $\mathfrak{B}$ of the relation structure $\mathfrak{A}$ of the language L is a subsystem of $\mathfrak{A}$ such that

$$\mathfrak{B} \models \varphi(b_0, \dots, b_n), \quad b_i \in B$$

if and only if

$$\mathfrak{A} \models \varphi(b_0, \dots, b_n)$$

for every formula φ of L .

Thus, in particular, the same set of sentences of L is valid in $\mathfrak{A}$ and $\mathfrak{B}$ so that $\mathfrak{A}$ and $\mathfrak{B}$ are models of the same complete theory. The fact that $\mathfrak{B}$ is an elementary submodel of $\mathfrak{A}$ is denoted by $\mathfrak{B} < \mathfrak{A}$. It can be shown that $\mathfrak{B} < \mathfrak{A}$ if for every formula φ of L

$$\mathfrak{A} \models \exists v_0 \varphi(v_0, b_1, \dots, b_n), \quad b_i \in B,$$

if and only if there is a $b_0 \in B$ such that

$$\mathfrak{A} \models \varphi(b_0, b_1, \dots, b_n).$$

Let B be any subset of the Skolem model $\mathfrak{A}^*$ of the language L^* . From the preceding paragraph and from the fact that a Skolem model satisfies the defining sentences of L^* , it follows that the subsystem generated by B in $\mathfrak{A}^*$ is an elementary submodel of the model $\mathfrak{A}^*$. This subsystem is the set of terms $\{t(b_0, \dots, b_n) : b_i \in B, t \text{ a Skolem term}\}$.

Now to finish off the Ehrenfeucht–Mostowsk theorem 1.1. In the proof of Theorem 2.4, assume T is a Skolem theory and $\mathfrak{B}$ a Skolem model. The model $\mathfrak{A}$ whose existence is asserted by Theorem 2.4 is now a Skolem model. The elementary submodel of $\mathfrak{A}$ generated by X is a (Skolem) model of T which satisfies all the conclusions of Theorem 1.1.

3.5. DEFINITION. The *elementary submodel* of the (Skolem) model $\mathfrak{A}$ of Theorem 2.4 generated by X is denoted by $\mathcal{M}(\Phi, X)$ where Φ is the E.–M. set of formulas in the language L^* satisfied by the properly ordered tuples of X .

We devote the rest of this section to some properties of the models $\mathcal{M}(\Phi, X)$.

(1) Every theory T has a model with a non-trivial automorphism.

Proof. Take for $\langle X, < \rangle$ a linear ordering such as the rationals which has a non-trivial order automorphism.

3.6. DEFINITION. A monomorphism f between the relation structures $\mathfrak{A}$ and $\mathfrak{B}$ of the language L

$$f : \mathfrak{A} \rightarrow \mathfrak{B}$$

is *elementary* if it has the property that for all formulas φ of L

$$\mathfrak{A} \models \varphi(a_0, \dots, a_n), \quad a_i \in A$$

if and only if $\mathfrak{B} \models \varphi(fa_0, \dots, fa_n)$.

(2) Consider two structures $\mathcal{M}(\Phi, X)$ and $\mathcal{M}(\Phi, Y)$.

(a) Any order preserving map f of X into Y induces an elementary map of $\mathcal{M}(\Phi, X)$ into $\mathcal{M}(\Phi, Y)$.

(b) The elementary monomorphism induced by f is surjective if and only if f maps X onto Y .

Proof. (a) Obvious since properly ordered tuples of X and Y satisfy the same formulas.

(b) Assume $y \in Y - f(X)$ and $y \in f(\mathcal{M}(\Phi, X))$. Then $y = t(fx_0, \dots, fx_m) = t(y_0, \dots, y_m)$ for some $x_0 < \dots < x_m \in X$ and $y_0 < \dots < y_m \in Y$, $y \neq y_i$, $0 \leq i \leq m$. Assume $y_0 < \dots < y_k < y < y_{k+1} < \dots < y_m$. Since Y is homogeneous with the E.-M. set Φ , the formulas

$$\begin{aligned} v_{k+1} &= t(v_0, \dots, v_k, v_{k+2}, \dots, v_{m+1}) \\ &= t(v_0, \dots, v_k, v_{l+1}, \dots, v_{l+m-k}) = v_l \end{aligned}$$

with $l \neq k+1$ are in Φ . But these formulas imply that Y contains at most $m+2$ distinct elements which contradicts the fact that Y is an infinite linear ordering. $\square$

4. ω -logic

An ω -logic is a language with a constant for every natural number and two sorts of variables; one sort ranges over the set of natural numbers, the other sort ranges over the universe. The set of variables which range over the natural numbers we enumerate as $w_0, w_1, \dots, w_n, \dots$; the other set of variables we enumerate as $v_0, v_1, \dots, v_n, \dots$. For more details, consult 5.2 of Chapter A.1. The results of this section apply equally well to weak second order logic, as defined in 5.3 of Chapter A.1.

Does the Ehrenfeucht–Mostowski theorem 1.1 generalize to ω -logic? Obviously there is no difficulty in adding Skolem functions to the language L of ω -logic to form the language L^* and in writing down defining sentences for them. The difficulty arises in the construction of the E.-M. set Φ of formulas. How do we deal with formulas of the form $\varphi \equiv \exists w_0 (t(v_0, \dots, v_n) = w_0)$? We must assign to $t(v_0, \dots, v_n)$, $v_0 < \dots < v_n$, some particular natural number w . In general, the formula φ will induce a partition P of $n+1$ -tuples into ω disjoint classes. Thus, in place of the Ramsey Theorem, an appeal to the Erdős–Rado theorem is necessary.

4.1. THEOREM. *Let T be a countable theory of an ω -logic L . If T has ω -models in all powers $\beth_\alpha$, $\alpha \in \omega_1$, then given any linearly ordered set $\langle X, < \rangle$, there is an ω -model $\mathfrak{A}$ of T , $X \subset A$, such that, in $\mathfrak{A}$, all properly ordered tuples of X satisfy the same set of formulas of L .*

PROOF. Assume T is a Skolem theory in the ω -logic L^* and the $\mathfrak{A}_\alpha$, $|\mathfrak{A}_\alpha| \geq \beth_\alpha$, are Skolem models. Linearly order each $\mathfrak{A}_\alpha$ and enumerate the formulas of L^* : $\varphi_0, \varphi_1, \dots, \varphi_n, \dots$. There are two cases to consider at the first step.

(1) $\varphi_0 \equiv \exists w_0 (t(v_0, \dots, v_n) = w_0)$. The formula φ_0 induces a partition P of $A_{\alpha+n}^{(n+1)}$ into ω -classes, one which is the set of properly ordered $n+1$ -tuples which satisfy $\varphi_0^{-1} \equiv \neg \varphi_0$, and ω order classes each of which is composed of properly ordered $n+1$ -tuples which satisfy the formula

$$\varphi_0^l \equiv \exists w_0 (t(v_0, \dots, v_n) = w_0) \wedge t(v_0, \dots, v_n) = l, \quad l \in \omega.$$

By the Erdős–Rado theorem, there is a set $C_{\alpha+n}^0 \subset A_{\alpha+n}$ homogeneous for P and $|C_{\alpha+n}^0| \geq \beth_\alpha$. The particular formula φ_0^k , $k \geq -1$, satisfied by the properly ordered $n+1$ -tuples of $C_{\alpha+n}^0$ depends on α , but since there are only ω choices and ω is not cofinal in ω_1 , there is a cofinal subsequence $\{B_\alpha^0, \alpha \in \omega_1\}$ of the sequence $\{C_\alpha^0, \alpha \in \omega_1\}$ such that for some $k \geq -1$, for all $\alpha < \omega$, the properly ordered $n+1$ -tuples of B_α^0 satisfy the same formula φ_0^k and $|B_\alpha^0| \geq \beth_\alpha$.

(2) $\varphi_0 \equiv \varphi_0(v_0, \dots, v_n)$ and φ_0 is not of the form $\exists w_0 (t(v_0, \dots, v_n) = w_0)$. The formula φ_0 induces a partition P of $A_{\alpha+n}^{n+1}$ into two disjoint classes, one composed of those properly ordered $n+1$ -tuples which satisfy the formula $\varphi_0^0 = \varphi_0$ and those which satisfy $\varphi_0^{-1} \equiv \neg \varphi_0$. By Erdős–Rado, there is a set $C_{\alpha+n}^0 \subset A_{\alpha+n}$ homogenous for P and $|C_{\alpha+n}^0| \geq \beth_\alpha$. Noting that 2 is not cofinal in ω_1 , we find a cofinal subsequence $\{B_\alpha^0, \alpha \in \omega_1\}$ of the sequence $\{C_\alpha^0, \alpha \in \omega_1\}$ such that the properly ordered $n+1$ -tuples of B_α^0 satisfy just one of the formulas $\varphi_0^0 \equiv \varphi_0$ or $\varphi_0^{-1} \equiv \neg \varphi_0$ for all $\alpha \in \omega_1$.

Continuing the induction, construct a set of sequences $\{\{B_\alpha^n, \alpha \in \omega_1\}, n \in \omega\}$ such that

(i) $|B_\alpha^n| \geq \beth_\alpha$,

(ii) $B_\alpha^{n+1} \subset B_\beta^n$ for some β and the set of ordinals

$$\{\beta: \exists \alpha \in \omega_1 (B_\alpha^{n+1} \subset B_\beta^n)\}$$

is cofinal in ω_1 .

(iii) There is $k \geq -1$ such that the properly ordered tuples of B_α^n , for all $\alpha \in \omega_1$, satisfy φ_n^k . Denote the formula φ_n^k by ψ_n .

The E.–M. set Φ constructed by this process is the set of formulas $\{\psi_n, n \in \omega\}$.

The conclusion of the proof of Theorem 4.1 is similar to that of Theorem 2.4. $\square$

The proof of Theorem 4.1 yields directly a form of the Ehrenfeucht–Mostowski theorem 1.1 for theories T of ω -logic.

Another non-elementary language is $L_{\omega_1\omega}$. The formulas of a language of this sort are built up by induction from the formulas of a predicate calculus by allowing countable conjunctions and disjunctions but only finite quantifications. No formula of $L_{\omega_1\omega}$ has more than a finite number of free variables.

Theories T which are sentences of $L_{\omega_1\omega}$ behave like theories of a countable ω -logic. This phenomenon is explained by the fact that a countable disjunction $\bigvee_{i \in \omega} \Phi_i(v_0, \dots, v_n)$ of formulas Φ_i of the predicate calculus can be replaced by the single formula $\exists w_0 \Phi(w_0, v_0, \dots, v_n)$ of ω -logic with $\phi(i, v_0, \dots, v_n) \equiv \Phi_i(v_0, \dots, v_n)$ and a countable conjunction $\bigwedge_{i \in \omega} \phi_i(v_0, \dots, v_n)$ by the single formula $\forall w_0 \phi_i(w_0, v_0, \dots, v_n)$ of ω -logic. Thus, Theorem 4.1 applies equally well to theories T which are sentences of $L_{\omega_1\omega}$.

5. Types and Ehrenfeucht–Mostowski models

The next two theorems have interesting applications to algebraic theories, two of which are discussed in this section.

5.1. DEFINITION. A *one-type* of a theory T of the language L is a maximal set $\{\varphi_i \equiv \varphi_i(v_0): \varphi_i \text{ a formula of } L\}$ of formulas consistent with T . An *n -type* of a theory T of the language L is a maximal set $\{\varphi_i \equiv \varphi_i(v_0, \dots, v_{n-1}): \varphi_i \text{ a formula of } L\}$ of formulas consistent with T . A *one-type* of a theory T of L with respect to a relation structure $\mathfrak{B}$ of L is a maximal set $\{\varphi_i(v_0, b_1, \dots, b_n): b_i \in B, \varphi_i \equiv \varphi_i(v_0, \dots, v_n) \text{ a formula of } L\}$ of formulas with parameters from B consistent with T .

5.2. THEOREM. *A countable theory T of the predicate calculus which has an infinite model has models $\mathfrak{A}$, in every infinite power κ , which contain only a countable number of types with respect to any countable subset of A .*

Note. It will follow from the proof of Theorem 5.2 that if T is a countable theory of ω -logic which has ω -models of power $> \beth_\alpha$ for all $\alpha \in \omega_1$, then T has ω -models $\mathfrak{A}$ in every infinite power κ which satisfy the conclusion of Theorem 5.2.

PROOF. We will show that if κ is an infinite cardinal and Φ is an E.-M. set of formulas for the Skolem theory T , then $\mathcal{M}(\Phi, \kappa)$ where κ is the set of ordinals $< \kappa$ contains only a countable number of types with respect to any of its countable subsets C . An element of $\mathcal{M}(\Phi, \kappa)$ corresponds to a Skolem term $t(\lambda_0, \dots, \lambda_n)$, $\lambda_i \in \kappa$, $\lambda_0 < \dots < \lambda_n$. The elements of the countable set C correspond to terms in which the λ_i are elements of some countable subset $C' \subset \kappa$. The set C' is called the support of C . With respect to C , the type of a given term $t(\lambda_0, \dots, \lambda_n)$ is determined by the term $t(v_0, \dots, v_n)$ and the order of the λ_i with respect to C' . The $C' \subset \kappa$ is well ordered; there are only a countable number of ways to interpolate a finite set into it. Since there are only countably many Skolem terms $t(v_0, \dots, v_n)$, there are only countably many types with respect to C . $\square$

5.3. THEOREM. *A countable theory T which has a definable infinite linear ordering has non-isomorphic models in every uncountable power.*

PROOF. Applying the theorem above, we need only produce models $\mathfrak{A}$ of power $\kappa \geq \omega_1$ which have an uncountable number of one-types with respect to a countable subset $C \subset A$. Assume T is a Skolem theory, let the linear ordering be defined by $\varphi(v_0, v_1)$ and let $(X, <)$ be a linearly ordered set of power ω_1 containing a dense countable subset W . For every element $x \in X$ add a constant to T and, also, the sentences $\varphi(x_0, x_1)$ if and only if $x_0 > x_1$. The expanded theory T_1 is finitely consistent and therefore has models in every uncountable power κ . Each model $\mathfrak{A}$ of T_1 contains uncountably many types with respect to the countable subset W since each $x \in X$ realizes a different cut with respect to W . $\square$

In MACINTYRE and SHELAH [to appear] there is a nice application of Theorem 5.1. They prove the existence in every uncountable power κ of non-isomorphic universal locally finite groups. The following material is taken from their paper.

5.4. DEFINITION. A group G is *universal locally finite* if

- (1) G is locally finite, i.e. every finitely generated subgroup is finite.
- (2) An isomorphic copy of every finite group is embedded in G .
- (3) If G_1 and G_2 are isomorphic finite subgroups of G , then there is an inner automorphism of G mapping G_1 onto G_2 .

It is known that there are universal locally finite groups of each infinite power κ . Any locally finite group of infinite power κ can be embedded in a

universal locally finite group of power λ for each $\lambda \geq \kappa$. All countable universal locally finite groups are isomorphic.

The theory of universal locally finite groups G is a sentence T of the language $L_{\omega_1\omega}$. The sentence T is obtained by

(i) enumerating the countable set of multiplication tables D_{G_i} of finite groups G_i and asserting that every finite subset of elements of G satisfy one of these tables and that for every D_{G_i} there is a finite subset of G which satisfies it,

(ii) asserting that if two finite subsets of G each satisfy the same D_{G_i} , then there is an inner automorphism of G carrying one of the subsets onto the other.

5.5. THEOREM. *There are non-isomorphic universal locally finite groups in every uncountable power κ .*

PROOF. The theory T of locally finite groups has been shown to be a sentence of $L_{\omega_1\omega}$. Since it is known that locally finite groups exist in all infinite powers, the conclusion of Theorem 5.2 applies to T . We will find a locally finite group Γ of power ω_1 which contains ω_1 different types with respect to some countable subset $C \subset \Gamma$. The group Γ is embeddable in a universal locally finite group of any power $\kappa \geq \omega_1$.

Let S_3 be the symmetric group on three elements. S_3 has two generators α and β , $\alpha^2 = l$, $\beta^3 = l$, $\alpha\beta \neq \beta\alpha$. The (complete) direct product H^* of κ copies of any finite group is locally finite. Hence S_3^* is locally finite. The group S_3^* contains the countable subset

$$C \equiv \{a_i : i \in \omega, a_i(n) = \alpha \text{ if } n = i, a_i(n) = l \text{ if } n \neq i\}.$$

Choose a set P of ω_1 distinct subsets of ω . The group S_3^* contains the set C_p ,

$$C_p = \{c_x(n) : c_x(n) = l \text{ if } n \in X, c_x(n) = \beta \text{ if } n \notin X\}.$$

Note that $C_x \cdot a_i = a_i \cdot C_x$ if and only if $i \in X$. Thus, for X, Y distinct elements of P , the subsets of elements of C with which C_X and C_Y commute are distinct with the result that, with respect to C , C_X and C_Y have different types. Let Γ be the group generated by the elements of C and C_p in S_3^* . The group Γ , as a subgroup of a locally finite group, is locally finite, has power ω_1 and contains ω_1 types with respect to the countable subset C . $\square$

We give a brief discussion of ω -stable theories, generally omitting proofs.

5.6. DEFINITION. A complete theory T is called κ -stable if the number of one-types realized in any model $\mathfrak{A}$ of T with respect to an arbitrary subset C of A , $|C| \leq \kappa$, is at most κ .

Note. It is easy to see that an equivalent definition results if “one-type” is replaced by “ n -type”, for any $n \geq 1$.

5.7. THEOREM. If T is ω -stable, then T is κ -stable for all κ , $\kappa \geq \omega$.

5.8. DEFINITION. Let $\mathfrak{A}$ be a relation structure, X a subset of A , and S_n the symmetric group on n -elements. An n -ary relation R is *connected* over X in $\mathfrak{A}$ if for any sequence $\langle x_0, \dots, x_{n-1} \rangle$ of n distinct elements of X , there is an $s \in S_n$ such that $\mathfrak{A} \models R(x_{s(0)}, \dots, x_{s(n-1)})$; it is *anti-symmetric* over X in $\mathfrak{A}$ if there is $s \in S_n$ such that $\mathfrak{A} \models \neg R(x_{s(0)}, \dots, x_{s(n-1)})$.

Note. If $\mathfrak{A} = \langle X, < \rangle$, then $<$ is an anti-symmetric connected binary relation over X .

5.9. THEOREM. No model $\mathfrak{A}$ of an ω -stable theory T contains an infinite subset X over which there exists an anti-symmetric connected relation R .

PROOF. A variant of Theorem 5.1. $\square$

5.10. DEFINITION. A linearly ordered set $\langle X, < \rangle$, X a subset of the relation structure $\mathfrak{A}$, is *homogeneous* with respect to the subset B of A if for all properly ordered tuples of X , $x_0 < \dots < x_n$ and $y_0 < \dots < y_n$, and all formulas $\varphi(v_0, v_1, \dots, v_n, \dots, v_{n+m})$ of L ,

$$\mathfrak{A} \models \varphi(x_0, \dots, x_n, b_{n+1}, \dots, b_{n+m})$$

if and only if

$$\mathfrak{A} \models \varphi(y_0, \dots, y_n, b_{n+1}, \dots, b_{n+m})$$

where the parameters b_i are arbitrary elements of B .

5.11. THEOREM. Let T be an ω -stable theory, κ a regular uncountable cardinal, $\mathfrak{A}$ a model of T of power κ and B any subset of A of power $< \kappa$. Then $\mathfrak{A}$ contains a subset X of power κ which is homogeneous with respect to B .

This theorem is remarkable in that it asserts that the model $\mathfrak{A}$ must contain a large homogenous set X . Using Theorem 5.9, it is possible to

show that the formulas satisfied by the tuples of X do not depend on their ordering. Thus, viewed in the context of the Ehrenfeucht–Mostowski theorem 1.1, the models $\mathcal{M}(\Phi, X)$ of ω -stable theories provide a complete analog to the example of free groups discussed in Section 1.

6. Partition theorems for large cardinals and the constructible universe

We introduce a partition theorem that will enable us to deduce the existence of an E.–M. set Φ such that $\mathcal{M}(\Phi, X)$ is well ordered if X is well ordered. This condition on Φ is necessary if we wish to apply results about the models $\mathcal{M}(\Phi, X)$ to set theory.

The notation $\kappa^{<\omega}$, κ a cardinal, $\kappa = \{\lambda, \lambda \text{ an ordinal } < \kappa\}$, refers to the set of all properly ordered finite sequences of κ .

6.1. DEFINITION. A subset Y of κ is *homogeneous* for a partition P of $\kappa^{<\omega}$ into disjoint sets if $Y^{(n)}$ is contained in one partition class for each n . The partition class may depend on n .

In this section our attention will center on cardinals κ such that $\kappa \rightarrow (\omega_1)_2^{<\omega}$. The existence of a cardinal κ with this property cannot be deduced from the axioms of ZFC. However, it does follow from these axioms that the first such cardinal is weakly compact, strongly inaccessible, and, indeed, larger than the least cardinal satisfying any of the combinatorial properties mentioned in the body of Chapter B.3. The following theorem is due to Rowbottom. A proof can be found in MORLEY [1968].

6.2. THEOREM. If $\kappa \rightarrow (\omega_1)_2^{<\omega}$, then $\kappa \rightarrow (\omega_1)_{2^\omega}^{<\omega}$.

6.3. THEOREM. Assume that $\kappa \rightarrow (\omega_1)_2^{<\omega}$ and that the theory T has a well ordered model $\mathfrak{A}$ of power κ . Then $\mathfrak{A}$ contains a homogenous set Y of power ω_1 and the E.–M. set Φ satisfied by the properly ordered tuples of Y has the property that if $\langle X, < \rangle$ is well ordered, the model $\mathcal{M}(\Phi, X)$ is well ordered.

PROOF. Assume that T is a Skolem theory and $\mathfrak{A}$ a Skolem model of T . Denote the well ordering of $\mathfrak{A}$ by $<$. The countable set of formulas of L^* induces a partition of $\mathfrak{A}^{<\omega}$ into 2^ω classes. There is a subset Y of power ω_1 of $\mathfrak{A}$ which is homogeneous for this partition. Let Φ be the set of formulas satisfied by the properly ordered tuples of Y .

Assume for some well ordered $\langle X, < \rangle$ that $\mathcal{M}(\Phi, X)$ is not well ordered.

$\mathcal{M}(\Phi, X)$ contains a countable descending chain $z_0 > z_1 > \cdots > z_n > \cdots$. The sequence $\{z_i, i \in \omega\}$ has a countable support $C \subset X$; every z_i is represented by some term $t(x_0, \dots, x_n)$, $x_i \in C$. Since C is a countable well ordered set, there is an order preserving map f of C into the homogenous set Y of power ω_1 , $Y \subset A$. The map f induces an elementary monomorphism of $\mathcal{M}(\Phi, C)$ into $\mathcal{M}(\Phi, Y)$. $\mathcal{M}(\Phi, Y)$ is an elementary submodel of A ; $\mathfrak{A}$ therefore contains a countable descending chain $fz_0 > fz_1 > \cdots > fz_n > \cdots$, contradicting the fact that $<$ well orders A .

6.4. THEOREM. *If the theory T satisfies the hypotheses of Theorem 6.3, then we can find an E.-M. set Ψ for T which, besides satisfying the conclusion of Theorem 6.3, has the property that for every Skolem term t , Ψ contains the formulas*

$$(1)_i \quad \begin{aligned} t(v_0, \dots, v_{m+n}) \leq v_m &\rightarrow t(v_0, \dots, v_{m+n}) \\ &= t(v_0, \dots, v_m, v_{m+n+1}, \dots, v_{m+2n}), \end{aligned}$$

$$(2)_i \quad \begin{aligned} v_n < t(v_0, \dots, v_{n-1}, v_{n+1}, \dots, v_m) &\rightarrow v_{n+1} \\ &\leq t(v_0, \dots, v_{n-1}, v_{n+1}, \dots, v_m). \end{aligned}$$

PROOF. Consider the model $\mathcal{M}(\Phi, \omega_1)$ where Φ is the E.-M. set whose existence is asserted in Theorem 6.3. Let P be the set of all homogenous subsets Y of power ω_1 contained in $\mathcal{M}(\Phi, \omega_1)$ and let $\Gamma = \{\lambda; \lambda \text{ is the } \omega\text{-th element of } Y \text{ with respect to the well ordering } < \text{ of } \mathcal{M}, Y \in P\}$. The minimum λ_ω of Γ exists and is an element of Γ . Let $Z \in P$ be a homogenous set whose ω -th element is λ_ω and let Ψ be the E.-M. set satisfied by properly ordered tuples of Z . $\square$

It is an exercise to show that if Ψ did not include the formulas (1)_i or (2)_i with respect to some Skolem term t , then t would give rise to set of power ω_1 homogenous for $\mathcal{M}(\Phi, \omega_1)$ whose ω -th term was strictly less than λ_ω .

Henceforth we assume familiarity with the usual axiom systems for set theory as discussed in Chapter B.1.

Suppose T is the usual set of axioms for Zermelo–Fraenkel set theory with choice (ZFC) plus the axiom of constructibility $V = L$. If T has a model whose ordinals have order type λ , $\lambda \geq \kappa$, $\kappa \rightarrow (\omega_1)_2^{<\omega}$, Theorem 6.3 asserts that $\mathfrak{A}$ contains a set of ordinals Y of power ω_1 which are homogenous for $\mathfrak{A}$. In this case, it is possible to prove the existence of an E.-M. set Ψ , called *remarkable*, which contains in addition to the formulas (1)_i and (2)_i of Theorem 6.4, the formulas

$$(3)_i \quad t(v_0, \dots, v_{n-1}) < v_n$$

for each Skolem term t of L^*

For a remarkable E.-M. set Ψ , the ordinals of the models $\mathcal{M}(\Psi, \kappa)$, κ an uncountable cardinal, are not only well ordered but actually have order type κ . Thus, by the Gödel isomorphisms theorem, $\mathcal{M}(\Psi, \kappa)$ is actually isomorphic to $\langle \{F(\alpha), \alpha < \kappa\}, \varepsilon \rangle$ when $F(\alpha)$ enumerates the set constructible at level α .

Using the reflection principle, it is easy to show that $\mathcal{M}(\Psi, \kappa)$, κ an uncountable cardinal, is actually an elementary subsystem of the constructible universe. In particular, $\mathcal{M}(\Psi, \omega_1)$ is an elementary subsystem of the constructible universe.

From the fact that Ψ is a remarkable E.-M. set, it follows that if α is a limit ordinal and $\beta > \alpha$, the ordinals of $\mathcal{M}(\Psi, \alpha)$ are an initial segment of the ordinals of $\mathcal{M}(\Psi, \beta)$. Thus the isomorphism between $\mathcal{M}(\Psi, \omega)$ and $\langle \{F(\alpha), \alpha < \omega\}, \varepsilon \rangle$ carries $\mathcal{M}(\Psi, \omega)$ onto $\langle \{F(\alpha), \alpha < \beta\}, \varepsilon \rangle$ for some countable limit ordinal β . But since $\mathcal{M}(\Psi, \omega) < \mathcal{M}(\Psi, \omega_1)$ and $\mathcal{M}(\Psi, \omega_1)$ is an elementary subsystem of the constructible universe L , it follows that $\langle \{F(\alpha), \alpha < \beta\}, \varepsilon \rangle$ is also an elementary subsystem of the constructible universe.

We are now in a position to draw some conclusions about the extent of the constructible universe L if the existence of a cardinal κ , $\kappa \rightarrow (\omega_1)_2^{<\omega}$ is assumed.

A definable element of the constructible universe L is necessarily a definable element of each of its elementary subsystems. In particular, every definable set of L is an element of the elementary subsystem $\langle \{F(\alpha), \alpha < \beta\}, \varepsilon \rangle$. But then, as viewed from the outside, every definable subset of L is countable. Thus the set of constructible subsets of ω is countable as seen from outside of L , though within L it has power ω_1 .

Using the techniques of Theorem 5.2, it is possible to show that the set of constructible subsets of any cardinal κ has power κ as viewed from outside of L . Of course, within L , the power set of κ is of power 2^κ . The constructible universe is small indeed and diverges sharply from the "real" world provided, of course, in this real world there is a cardinal κ , $\kappa \rightarrow (\omega_1)_2^{<\omega}$.

Recall that the formulas of the language of ZF can be effectively coded into the natural numbers. The set of integers corresponding to the remarkable E.-M. set Ψ is called 0^* in the literature. Of course 0^* is not a constructible set. The existence of the large cardinal κ , $\kappa \rightarrow (\omega_1)_2^{<\omega}$, implies that a relatively simple set of integers 0^* is not constructible. On the other

hand, if we assume the existence of the countable combinatorial property that the set of integers $0^\#$ exhibits, we are led to the conclusions concerning the size of the constructible universe. The existence of $0^\#$, a countable combinatorial property, places sharp bounds on the extent of the constructible universe. For more on this subject see SILVER [1973].

References

CHANG, C.C. and H.J. KEISLER

[1973] *Model Theory* (North-Holland, Amsterdam).

MACINTYRE, A. and S. SHELAH

[to appear] Uncountable universal locally finite groups.

MORLEY, M.

[1967] Partitions and models, in: *Proceedings of the Summer School in Logic, Leeds 1967*, edited by M.H. Löb, Lecture Notes in Mathematics, Vol. 70 (Springer, Berlin).

SILVER, J.

[1973] The bearing of large cardinals on constructibility, in: *Studies in Model Theory*, edited by M. Morley (Math. Assoc. Am., Buffalo, NY).

*Infinitesimal Analysis of Curves
and Surfaces*

K. D. STROYAN

Contents

1. Robinson's formulation of Leibniz' Principle	198
2. Elements of infinitesimal calculus	208
3. Continuous curvature and differentials	217
4. Kissing curves	221
5. Gauss' investigations of surfaces	225
References	230

1. Robinson's formulation of Leibniz' Principle

The intuitive notions of infinitely large and infinitesimally small numbers appeal to most people. These notions in one form or another were fundamental concepts in differential and integral calculus for about two hundred years after its invention by Newton and Leibniz. The notion of an infinitesimal number was recently put on a sound basis and in a way which retains the intuitive appeal of such numbers without contradiction. In this article we give some basic applications of infinitesimals in the study of the geometry of curves and surfaces. This provides rigorous arguments in the clear geometric style of Gauss. Moreover, we feel this approach hints at an insight of Riemann and others which may seem surprising to the modern mathematician, namely, that uniform curvature conditions are a very direct way to approach the now-common " C^1 " assumptions. The uniform smoothness conditions for the first derivative are so simple and natural that they could easily be used at a freshman level avoiding a certain amount of technicality in the usual approach. Finally, modern differential forms can be obtained by a factorization in the infinitesimals providing a direct link to Gauss — the infinitesimal approach can be automatically "modernized".

Introduction of infinitesimals into mathematics in the late seventeenth century was a source of great controversy, one which was not resolved mathematically until 1960. The resolution may not yet be widely understood. In the late eighteenth century, d'Alembert attempted to base calculus on the notion of limit in order to resolve the difficulty. In the late nineteenth century, thru the research and influence of Weierstrass, the "epsilon-delta" method, akin to the ancient Greek "method of exhaustion", became the fundamental "limiting" technique of analysis. Bolzano had proposed the method some fifty years earlier, but was largely ignored. Cauchy's systematic use of limits, which he defined using infinitesimals, provided a link between the position of De l'Hôpital, the author of the first calculus text who treated infinitesimals as a metaphysical fact, and that of Weierstrass. The "epsilon-delta" method reigned so supreme in the years following Weierstrass, that there seemed to be a feeling that infinitesimals could not be treated consistently. Leibniz' approach ultimately was vindicated.

In 1961, Abraham Robinson gave a precise formulation of the metamathematical principle which Leibniz proposed to govern the infinitesimals (ROBINSON [1961]). Leibniz considered the infinitesimals to be a "useful fiction" rather than a metaphysical fact but was concerned with the rules which they obey. He stated the principle that the "ideal numbers"

were to have the same properties as the “finite numbers” and vice versa, but he was not specific as to which properties this was to apply. For example, there is a clear contradiction with the completeness axiom or the well ordering of the natural numbers. The modern logician will recognize these examples as troublesome “higher order” formulas — ones with quantifiers over sets rather than only numbers. The Archimedean axiom provides an even more compelling problem to which Leibniz did not address himself. The tools of modern model theory, which studies the relationship between formal languages and mathematical structures, provide a framework in which Robinson could formulate Leibniz' principle.

A formal language of ordinary analysis has an interpretation in a nonstandard model by virtue of the Gödel Completeness Theorem or the Compactness Theorem (see Proposition 2.7 in Chapter A.1, for example). Nonstandard extensions also can be exhibited by the ultrapower method discussed in Chapter A.3.

A simple algebraic theorem says that once one has a proper ordered field extension of the real numbers, the extension is non-Archimedean, that is, contains infinitesimals and their infinite reciprocals. Moreover, a formal sentence whose interpretation in the standard model is true has a true interpretation in the nonstandard model and vice versa. This is the rule of Leibniz, but there is a difficulty — why doesn't the Archimedean property hold in the nonstandard model contrary to our algebraic reasoning above? Or more technically: How can you apply the Compactness Principle to a higher order language? The answer is that Robinson uses a first order language for higher order formal analysis and the interpretation of higher order sentences in the nonstandard model is subsequently weaker than the informal meaning. But how can a first order theory be useful in analysis ...?

We shall sketch the idea here and reinforce it with examples. The only formal subtlety is the care one must exercise with quantifiers. First of all, “for all x ” and “there exists y ” are not permitted — only bounded quantifiers are allowed, e.g., “for every positive ε in $\mathbb{R}$ ” and “there exists an element n in $\mathbb{N}$ ”. The real tricky part of this in the nonstandard model is that quantifiers over sets are specified to run over a particular set of sets. All the sets which come up in classical analysis have nonstandard extensions by a map denoted “ $*$ ”. One obtains Leibniz' transferred property by applying $*$ to each set in a sentence — this is called *the $*$ -transform*. First order properties transfer identically, but higher order properties have restrictions on their quantifiers — only *internal sets* lie in the scope of a transformed quantifier.

One suitable definition of “all the sets which arise in classical analysis” begins by defining a superstructure over a set of atoms (or urelements)

X_0 , an infinite set of atoms

$$X_{k+1} = \mathcal{P} \left(\bigcup_{n=0}^k X_n \right), \quad k \in \mathbb{N},$$

finally,

$$\mathcal{X} = \bigcup_{k \in \mathbb{N}} X_k.$$

We shall begin by looking at the case where $X_0 = \mathbb{R}$, the real numbers (as a set of atoms). Later we need to construct a superstructure $\mathcal{Y}$ on another set of atoms. Real valued functions are *elements* of $\mathcal{X}$, since functions “are” sets of ordered pairs and ordered pairs “are” sets $\{\{a\}, \{a, b\}\}$. The euclidean spaces $\mathbb{R}^n$ and all their subsets are also in $\mathcal{X}$ as elements. The classical spaces $\ell^2(\mathbb{N})$, $L^p[0, 1]$, $H^\infty(U)$, and so on, all are elements of $\mathcal{X}$.

Elements of $\mathcal{X}$ are called *entities* and the set theory of entities provides a framework for classical analysis. The algebraic object $(\mathcal{X}, \in)$ is called a *superstructure*. The bounded first order language of $\in$ describes the set theory of entities where we always have

$$\forall x [X \in A \Rightarrow \dots] \quad \text{or} \quad \exists y [y \in B \& \dots]$$

with A and B entities of $\mathcal{X}$. We have one constant in our language $L(\in)$ for each element of $\mathcal{X}$. These constants in turn have interpretations back in $\mathcal{X}$, for example, ρ of L might stand for $\mathbb{R} \in \mathcal{X}$ and we name the standard interpretation map “ I ”, $I(\rho) = \mathbb{R}$ in this case. We may think of any property of analysis expressed in terms of set theory and thus in terms of the relations $\in$ and $=$ of the superstructure. This is what we apply nonstandard extension to.

1.1. LEIBNIZ’ PRINCIPLE. *There is a set of atoms Y_0 and a mapping $*: \mathcal{X} \rightarrow \mathcal{Y}$, $\mathcal{Y}$ being the superstructure based on Y_0 , with the following properties:*

- (i) $*\mathbb{R} = Y_0$, the map applied to the ground set entity in $\mathcal{X}$ is the ground set in $\mathcal{Y}$.
- (ii) The extension is proper, the hyperreal numbers $*\mathbb{R}$ properly contain the standard embedded reals ${}^\circ\mathbb{R} = \{*r: r \in \mathbb{R}\}$, in particular, there is a nonzero infinitesimal in $*\mathbb{R}$.

(iii) Every sentence about $\mathcal{X}$ with a bounded formalization in the language of $\in$ holds in $\mathcal{X}$ if and only if the $*$ -transform obtained by extending each constant of the sentence holds in the range $*\mathcal{X}$.

PROOF. Apply the Compactness Theorem (Theorem 2.4 in Chapter A.1) to the set of sentences of $L(\in)$ whose interpretation in $\mathcal{X}$ is true plus the infinite set of sentences saying $c \in I^{-1}(\mathbb{R})$ but $\{c \neq I^{-1}(r) : r \in \mathbb{R}\}$, where “ c ” is a new constant which has not already been used. Altogether these formulas are finitely satisfiable, thus have a model $\mathcal{M}$. (Alternate to Compactness we may apply the Fundamental Theorem on ultraproducts from Chapter A.3 to obtain the same result.)

Now we apply the Mostowski collapsing of the well-founded portion of $\mathcal{M}$ (see 3.7 in Chapter A.7 for example). This gives us a ground set ${}^*\mathbb{R}$ as the collapsed interpretation of the constant $I^{-1}(\mathbb{R})$. The rest of the collapsing of $\mathcal{M}$ lies inside the superstructure on ${}^*\mathbb{R}$. Bounded formulas only refer to this part, so our theorem is proved. Collapsing is shown in Fig. 1.

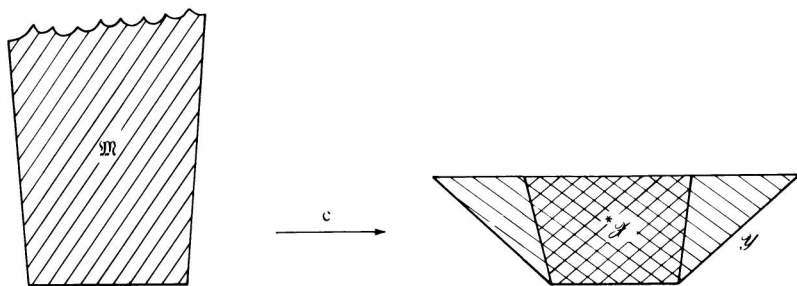


Fig. 1. A picture of ${}^*\mathcal{X}$ showing “infinite types” chopped off and external part of $\mathcal{Y}$

We view the nonstandard model ${}^*\mathcal{X}$ of our language as a *proper elementary extension* of $\mathcal{X}$ (with respect to the bounded quantifier formulas) embedded in the superstructure $\mathcal{Y}$ based on the hyperreals ${}^*\mathbb{R}$. It is important that we embed ${}^*\mathcal{X}$, that is, have “real” $\in$ as the interpretation in the nonstandard model, in order to be able to deal with both internal and external sets. All the new constructions will be based on external sets, yet involve important interactions with internal ones. $\square$

Now we give some examples and consequences of Leibniz' Principle. A first order example is *commutativity of addition*:

$$I\{\forall x \forall y [(x \in \rho \& y \in \rho) \Rightarrow (x + y = y + x)]\}, \quad \text{where } I(\rho) = \mathbb{R},$$

“for every x and y in the reals $\mathbb{R}$, $x + y$ equals $y + x$ ”. The $*$ -transform is:

$$I'\{\forall x \forall y [(x \in \rho \& y \in \rho) \Rightarrow (x + y = y + x)]\}, \quad \text{where } I'(\rho) = {}^*\mathbb{R},$$

“for every x and y in the hyperreals ${}^*\mathbb{R}$, $x + y$ equals $y + x$ ”. In a like manner, *all the first order ordered field axioms transfer to ${}^*\mathbb{R}$* . Notice that we

have extended addition, which can be thought of as a ternary relation $S = \{(x, y, z): x + y = z; x, y, z \in \mathbb{R}\}$. It is customary not to write a star on operations like $+$, $\cdot$, $\leq$, or on standard functions, since the extension agrees on standard points.

The *Archimedean axiom*, “for every positive real x , there is a natural number n , such that $x > 1/n$ ”,

$$I\{\forall x \exists n [x \in \mathbb{R} \Rightarrow [n \in \mathbb{N} \& [x > 1/n]]]\},$$

transforms to

$$I'\{\forall x \exists n [x \in {}^*\mathbb{R} \Rightarrow [n \in {}^*\mathbb{N} \& [x > 1/n]]]\},$$

by abuse of notation involving the constant for $\mathbb{R}$ and ${}^*\mathbb{R}$, $\mathbb{N}$ and ${}^*\mathbb{N}$, the less than, and division, “every positive hyperreal x is smaller than $1/n$ for some positive *hyperinteger*”. By being forced to extend the bounds on the existential quantifier we do *not* obtain Archimedes’ axiom, but rather that each infinitesimal is more than the reciprocal of some *infinite integer* of ${}^*\mathbb{N}$, the extension of the set of natural numbers. The numbers 1, 2, 3, etc., from $\mathbb{N}$ each have a unique extension in ${}^*\mathbb{N}$, we call the embedded standard set ${}^\sigma\mathbb{N} = \{{}^*n: n \in \mathbb{N}\}$ and usually do not bother to write *1 , *2 , etc., for familiar numbers. The point we wish to make is that

$${}^*\mathbb{N}_\infty = {}^*\mathbb{N} - {}^\sigma\mathbb{N} \neq \emptyset,$$

there are infinite numbers in ${}^*\mathbb{N}$. In fact, every infinite set A from classical analysis is properly extended:

$${}^*A - {}^\sigma A \neq \emptyset,$$

where *A is the extension of the set.

The set

$${}^\sigma A = \{{}^*a: a \in A\}$$

is the (externally) embedded standard set. We explore this further in the next example.

1.2. DEFINITION. The *infinitesimals* are given by:

$$o = \{x \in {}^*\mathbb{R}: |x| < 1/n \text{ for each } n \in {}^\sigma\mathbb{N}\}.$$

We write $x \approx y$ if $(x - y) \in o$ and say x is infinitesimally close to y . The ring of *finite numbers* is given by:

$$\mathcal{O} = \{x \in {}^*\mathbb{R}: |x| < n \text{ for some } n \in {}^\sigma\mathbb{N}\}.$$

The *infinite numbers* by ${}^*\mathbb{R}_\infty = {}^*\mathbb{R} - \mathcal{O}$.

Besides “infinitesimally close” we may also say “infinitely near” or

simply “nearly”. We say a hyperreal b is “*near-standard*” if there is an $a \in {}^\sigma\mathbb{R}$ with $a \approx b$.

Since ${}^*\mathbb{N} - {}^\sigma\mathbb{N} \neq \emptyset$ there exist infinite integers $\Omega, \Omega + 1, 3 \cdot \Omega, \Omega^2, \Omega^n$. All these are different by Leibniz' Principle, for example, “for every $x \in \mathbb{R}$, $x + 1 \neq x$ ” says $\Omega + 1 \neq \Omega$, and so on. (Observe therefore that neither cardinal nor ordinal numbers in Cantor's sense can serve as ${}^*\mathbb{N}$.) The reciprocals $1/\Omega, 1/\Omega^n$ are infinitesimal.

One can summarize the properties of finite and infinitesimal numbers algebraically by:

1.3. THEOREM. *$\mathcal{O}$ is an ordered ring containing o as a maximal order ideal and $\mathcal{O}/\approx$ is order isomorphic to $\mathbb{R}$, that is, each finite hyperreal is infinitesimally near its standard part in ${}^\sigma\mathbb{R}$. We denote the canonical homomorphism by “st”,*

$$o \rightarrow \mathcal{O} \xrightarrow{\text{st}} \mathbb{R},$$

or sometimes, $\hat{a} = \text{st}(a)$.

We shall omit the proof, see ROBINSON [1966] or STROYAN and LUXEMBURG [1976]. One important observation from this is the fact that a *finite number times an infinitesimal is infinitesimal*. The theorem gives a useful picture, which KEISLER [1976] calls the *Infinitesimal Microscope* (see Fig. 2).

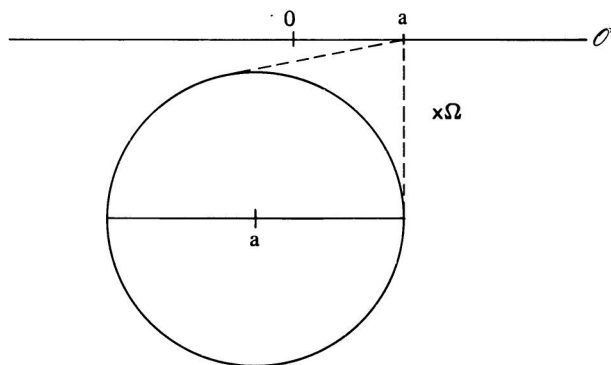


Fig. 2. Infinitesimal Microscope: “ a ” is the only standard number in the field of view

Two points in ${}^*\mathbb{R}$ are finitely far apart if $(x - y) \in \mathcal{O}$. For example, the integers $\Omega, \Omega \pm 1, \Omega \pm 2$, and $\Omega \pm n$ for $n \in {}^\sigma\mathbb{N}$ are finitely far apart.

Notice that Ω/n for $n \in {}^\sigma\mathbb{N}$ is infinite and infinitely far from Ω as is $n \cdot \Omega$ and Ω^n . The *Infinite Telescope* says that each *galaxy* or finite equivalence class looks like a copy of $\mathcal{O}$. This follows from Leibniz' Principle applied to "translation is an isometry" plus the last theorem to describe $\mathcal{O}$.

Our final example of a $*$ -transform is as follows. *Completeness of $\mathbb{R}$* says "every set B in the power set of $\mathbb{R}$ which is bounded above has a least upper bound",

$$I\{\forall B[(B \in \mathcal{P}(\mathbb{R}) \& \exists y[y \in \mathbb{R} \& \forall x[x \in B \Rightarrow x < y]]] \Rightarrow \\ \exists b[b \in \mathbb{R} \& \forall z[z \in \mathbb{R} \Rightarrow [\forall w[w \in B \Rightarrow w < z] \Rightarrow b \leq z]]]\}.$$

The constants of the formal sentence are really $I^{-1}(\mathcal{P}(\mathbb{R}))$ and $I^{-1}(\mathbb{R})$, $I^{-1}(<)$ and $I^{-1}(\leq)$. The $*$ -transform says that every set $B \in {}^*\mathcal{P}(\mathbb{R})$ which has an upper bound has a least upper bound. *Not every subset of ${}^*\mathbb{R}$ arises in ${}^*\mathcal{P}(\mathbb{R})$* ; we have the following inclusions, all strict:

$${}^\sigma\mathcal{P}(\mathbb{R}) \subset {}^*\mathcal{P}(\mathbb{R}) \subset \mathcal{P}({}^*\mathbb{R}).$$

In other words, $*$ -completeness is not the same as completeness in ${}^*\mathbb{R}$. *The set of infinitesimals has no least upper bound*, since half a finite number is still an upper bound and twice an infinitesimal exceeds the original (using Leibniz' Principle on the sentence "for every positive $x \in \mathbb{R}$, $2x > x$ "). Hence,

$$o \notin {}^*\mathcal{P}(\mathbb{R}),$$

of course,

$$o \in \mathcal{P}({}^*\mathbb{R}),$$

the infinitesimals are a subset of the hyperreals.

1.4. DEFINITION. If A is an entity in $\mathcal{X}$, both A and its extension *A are referred to as *standard* sets. The standard sets are elements of ${}^\sigma\mathcal{P}(X_k)$ for some $k \in \mathbb{N}$.

Elements $B \in {}^*\mathcal{A}$ of standard sets ${}^*\mathcal{A}$ are said to be *internal*. For example, internal subsets of ${}^*\mathbb{R}$ are the elements of ${}^*\mathcal{P}(\mathbb{R})$. The set

$$\{x \in {}^*\mathbb{R}: x \geq \Omega\} = [\Omega, \infty)$$

is an internal set in ${}^*\mathcal{P}(\mathbb{R})$ and not in ${}^\sigma\mathcal{P}(\mathbb{R})$ when Ω is infinite. This is internal by Leibniz' Principle applied to the statement "for every $a \in \mathbb{R}$, $[a, \infty) \in \mathcal{P}(\mathbb{R})$ ". The internal sets are the ones which the formal language "knows about"; any formal property referring only to internal sets itself describes an internal set. The symbol " ∞ " is *not* a hyperreal number.

The remaining sets in the superstructure based on ${}^*\mathbb{R}$ are called *external*.

We proved that *the infinitesimals are external*, that is, $o \in \mathcal{P}({}^*\mathbb{R}) - ({}^*\mathcal{P}(\mathbb{R}))$. Observe that existence of external sets in our model requires us to embed ${}^*\mathcal{X}$ in set theory (or deal simultaneously with internal sets in two set theories). This is the difference between an infinitesimal analysis nonstandard model and the standard nonstandard models of set theory (which need not be “well founded”).

The space of continuous functions $C[0, 1]$ extends to the * -continuous functions ${}^*C[0, 1]$, that is, Leibniz' Principle says each $f \in {}^*C[0, 1]$ is a real valued function on the set $\{x \in {}^*\mathbb{R}: 0 \leq x \leq 1\} = {}^*[0, 1]$. The * -continuous functions satisfy the * -transform of epsilon-delta continuity.

The interaction between internal and external sets is what makes Robinson's theory fruitful. As a final example, consider the internal function $f(x) = \sin(\pi\Omega x)$ for infinite $\Omega \in {}^*\mathbb{N}_\infty$. We know f is * -continuous: “for every $n \in {}^*\mathbb{N}$, $\sin(\pi nx) \in {}^*C[0, 1]$ ”, Would you say it is continuous in the standard sense? What is $f(0)$? $f(\frac{1}{2}\Omega)$?

We will use this formulation of “ideal numbers” to sketch Infinitesimal Calculus à la Leibniz–Robinson and develop Infinitesimal Geometry à la Gauss afterward, but first we close the section by trying to place Robinson's contribution in historical perspective. We strongly encourage our reader to consult, in ROBINSON [1966], Robinson's own account of the history of calculus. It is our belief that Robinson's solution of Leibniz' problem stands as one of the major results of twentieth-century mathematics. After nearly three centuries, Robinson put the original intuitive formulation of calculus on as sound a basis as the rest of modern mathematics. It is our belief that infinitesimal methods will prove useful in modern pure and applied mathematics as well, there is strong evidence that infinitesimals and * -finite sets can aid the art of invention by making various complicated limits more clear and intuitive.

While Leibniz felt that the ideal numbers ought to have a consistent treatment he was both aware of contradictions and stated that infinitesimal arguments could be replaced by arguments “in the style of Archimedes”. A precise formulation of the latter assertion is an open problem, see ROBINSON [1973], problem eleven. As to the inconsistency, Newton's fluxions also suffered. BERKELEY [1734] gave an excellent account of the difficulties associated with throwing away “higher order terms” and maintaining equality (see also NEWMAN [1956]). This led him to call infinitesimals “ghosts of departed quantities”. Berkeley showed that the fluxions were no more consistent. With hindsight we cannot help but wonder why the equivalence “is infinitesimally close to” was not distinguished from “is equal to”. Besides the infinitesimal relation “ $\approx$ ” of (1.2)

above, we shall see that relative infinitesimals on a scale of another infinitesimal play a fundamental role in Gaussian infinitesimal geometry. These correspond to throwing away “second order terms” and keeping “first order terms”

Leibniz' methods brought about tremendous development of calculus and to some extent for a time the results overshadowed the underlying inconsistencies. Nevertheless, Euler, for one, checked his results by numerous methods because of his openly expressed scepticism. His great care and insight is reflected in the fact that his *proof* of one of his most fundamental lemmas, the product formula for $\sin(x)$, has been given a translation into Robinson's theory of infinitesimals and stands as correct! (See LUXEMBURG [1973] and STROYAN [1976].)

Both Lagrange and d'Alembert attempted to banish infinitesimals and solve the foundational question around the end of the eighteenth century. By this time Leibniz' assertion that infinitesimal arguments could be rephrased into the style of Archimedes was not so obvious, but even after Weierstrass introduced “ ε - δ ” Riemann considered both methods correct, though Weierstrass' the more “concrete”. Besides intrinsic interest in the foundational question, analysis was sophisticated by the late nineteenth century, so sharp distinctions between convergence and uniform convergence and between continuity and uniform continuity were needed especially for trigonometric series and the calculus of variations. It is interesting to note that Riemann equated *uniform continuity* with Cauchy's

$$x \approx y \text{ implies } f(x) \approx f(y)$$

and that in 1853 Cauchy was forced to modify his infinitesimal definition of convergence from 1821 to a form which excluded a counterexample of Abel from 1826. Cauchy had proved that a series of continuous functions has a continuous limit. ROBINSON [1966], p. 273, shows that the revised form is equivalent to uniform convergence and indeed gives a correct result. We shall have use for a related simple notion of “uniformly differentiable”, which is equivalent to “continuously differentiable” and which shows that *Gauss' definition of a surface with “continuous curvature” actually means “C¹-embedded” in modern terminology*. The “surprisingly” stronger properties obtained by varying two things infinitesimally is one strength of Robinson's method.

About the same time that Weierstrass established “ ε - δ ”, Cantor created his theory of cardinal and ordinal numbers, again being motivated to an extent by questions from trigonometric series. Cantor's infinite numbers violate Leibniz' Principle so that the infinite numbers of Robinson

are a completely disjoint theory, though this fact certainly implies no conflict. The great progress in measure theory and topology brought about by Cantor's theory no doubt has contributed to modern disfavor for infinitesimals, but this success does not imply that there is only one kind of infinite number. We hope the mathematical community will recognize the existence of (at least) two kinds of infinite numbers.

The author is not qualified to comment on the philosophical implications of Robinson's contribution, but refers the reader at least to the closing remarks in ROBINSON [1973].

In the years since Robinson's vindication of infinitesimals, his ideas have been developed in several ways. KEISLER [1976] has given a simple axiomatic development of infinitesimals suitable for beginning calculus students. Keisler's approach to calculus largely avoids formal logic and provides a clear consistent introduction to calculus with the strong intuitive flavor infinitesimals have always had. His book also treats "epsilon-delta" where it arises naturally and essentially — in numerical approximation. Moreover, students' computational skills are enhanced by having infinitesimals. JENSEN [1972] has given a computer-oriented version of infinitesimal calculus where infinitesimals are infinitely accurate computations of an ideal machine. The investigation of SULLIVAN [1974] uses Keisler's approach for a broad spectrum of students and indicates that it is an exciting and practical educational endeavor.

Many researchers, especially Robinson himself, have shown how infinitesimals play a role in modern algebra and analysis. Two monographs, ROBINSON [1966] and STROYAN [1976], treat a wide spectrum of analysis from the point of view of infinitesimals. One important part of this research is in seeing how topics invented since "epsilon-delta" can be treated infinitesimally; this process frequently provides a new clear perspective. For example, in 1969 Behrens cast recent work on bounded holomorphic functions in terms of infinitesimals and subsequently made remarkable progress on the study of analytic structure of maximal ideals and on the Corona Problem. In BEHRENS [1974a] Behrens sketches the infinitesimal approach to that work and makes interesting new conjectures. There are other examples of this in the monographs cited above and in three symposium publications, LUXEMBURG [1969], LUXEMBURG and ROBINSON [1972], and HURD and LOEB [1974], as well as the notes of MACHOVER and HIRSCHFELD [1969] and the mathematical literature (JOHNSON [1975]). We are certain that experts in many fields would find the process of reformulating open problems in terms of Robinson's infinitesimal foundations rewarding as well as fun. Since infinitesimals frequently simplify compli-

cated “limiting procedures”, sustained hard work may also show that a formerly unsolvable problem lies within our grasp. We expect that process to require insight and effort, but we also expect that in many cases it will lead to significant progress if seriously attempted.

2. Elements of infinitesimal calculus

We begin our development of calculus by showing that “C¹” can be defined directly in a simple fashion. The “epsilon-delta” version of this theorem is “well known” but inadequately appreciated, in our opinion. In fact the property of uniform differentiability underlies a great deal of both differential and integral calculus. We begin with a global one-dimensional version to focus on the primary ingredient.

2.1. THEOREM. *Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a standard real valued function. The following are equivalent:*

(i) *There is a standard map $Df: \mathbb{R} \rightarrow \mathbb{R}$ such that whenever x is finite in ${}^*\mathbb{R}$ and whenever δz is a nonzero infinitesimal in ${}^*\mathbb{R}$,*

$$\frac{1}{\delta z} [f(x + \delta z) - f(x)] \approx (Df)_x.$$

(This is called uniform differentiability.)

(ii) *For each standard $a \in {}^\sigma\mathbb{R}$, there is a finite number Δ_a such that whenever $x \approx y \approx a$ in ${}^*\mathbb{R}$, $x \neq y$,*

$$\frac{f(y) - f(x)}{y - x} \approx \Delta_a.$$

(This is called local uniform differentiability at a .)

(iii) *The function f is continuously differentiable in the epsilon-delta sense.*

Condition (i) will be most useful to us in infinitesimal geometry. It is also the main ingredient in the proof of the Fundamental Theorem we give; that proof is essentially the same as Cauchy’s. The same idea underlies the change of variables, divergence, de Rham’s and other theorems that require “C¹” assumptions. It is closely related to the local flow or infinitesimal transformation of a “C¹” vector field as well (thru the “C¹-Picard” theorem).

The picture for condition (ii) under an infinitesimal microscope is shown in Fig. 3.

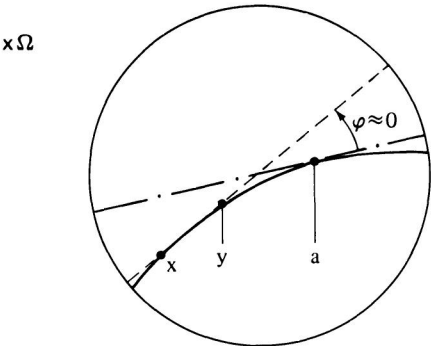


Fig. 3. Uniform differentiability at a under infinitesimal microscope.

Condition (ii) is a weaker requirement in the sense that we could ask that it is satisfied at a single point $a \in {}^\sigma\mathbb{R}$. BEHRENS [1974b] and NIJENHUIS [1974] show that this condition *at a single point* can replace the C^1 assumption of the inverse mapping theorem. Also, uniform partial derivatives imply uniform total derivatives. Condition (ii) is perhaps easiest to give an epsilon-delta formulation to — we leave that as an exercise.

The function $x^2 \sin(\pi/x)$ is not uniformly differentiable at zero. When $y = 1/(\Omega - \frac{1}{2})$ and $x = 1/\Omega$, $\Delta y/\Delta x \approx \pm 2$, $Df_x = \pm \pi$, and $Df_0 = 0$, as the reader can verify by calculations using Leibniz' Principle. This example points out dramatically that it does not suffice to check the conditions for a single value of δz or only for $x = a$ (but this is a small price to pay for consistent infinitesimals). The reader is also asked to draw $g(x) = |x|$ under an infinitesimal microscope at $x = 0$.

Notice that by direct calculation, $(f(\delta z) - f(0))/\delta z \approx 0$ for all infinitesimal δz in this example (see Fig. 4; zero is not shown this figure). Compare this with Theorem 2.2.

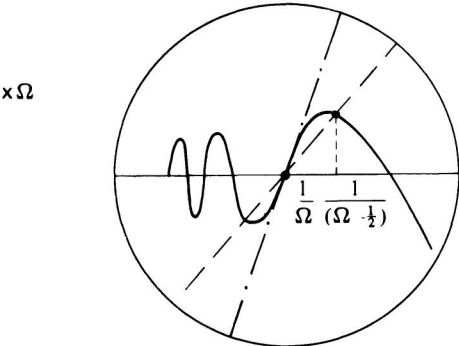


Fig. 4. Infinitesimal secants and tangents of $x^2 \sin(\pi/x)$

PROOF OF THEOREM 2.1. Let x be given infinitesimally close to $a \in {}^\sigma\mathbb{R}$. First we show that (i) implies $Df_x \approx Df_a$. Let z be a finite number and $\delta = |x - a|$ while δz is “ δ times z ”. Condition (i) at x says:

$$f(x + \delta z) - f(x) = Df_x \cdot \delta z + \delta \cdot \eta$$

for some $\eta \approx 0$. We may also apply the condition at a to obtain:

$$\begin{aligned} f(x + \delta z) - f(a) + f(a) - f(x) &= Df_a \cdot (x + \delta z - a) - Df_a \cdot (x - a) + \delta \cdot \zeta \\ &= Df_a \cdot \delta z + \delta \cdot \zeta, \quad \text{with } \zeta \approx 0. \end{aligned}$$

Now we subtract these two equations and divide by δz to see that

$$Df_x \approx Df_a.$$

Condition (ii) follows from this since

$$\frac{f(y) - f(x)}{y - x} \approx Df_x \approx Df_a$$

and Df_a is necessarily a standard number since it is the value of a standard function at a standard point. This shows that (i) implies (ii).

We divide the proof that (ii) implies (iii) into several steps. Theorems 2.2 and 2.3 are proved below.

2.2. THEOREM. *Let f be a standard real-valued function and $a \in {}^\sigma\mathbb{R}$. The following are equivalent:*

(i)(in ${}^*\mathbb{R}$) *There is a standard constant b such that whenever $x \approx a$ in ${}^*\mathbb{R}$, then $(f(x) - f(a))/(x - a) \approx b$.*

(ii)(in $\mathbb{R}$) *The function f is defined on a neighborhood of a and there exists a number $b \in \mathbb{R}$ satisfying the condition that for every $\varepsilon \in \mathbb{R}^+$, there is a $\delta \in \mathbb{R}^+$ such that whenever $|x - a| < \delta$, then $|(f(x) - f(a))/(x - a) - b| < \varepsilon$.*

Theorem 2.2 shows that f is epsilon-delta differentiable using condition (ii) with one number x or y set equal to a and the constant $b = \text{st}(\Delta_a)$. Moreover, we may use this to (externally) define a standard map $Df_a = \text{st}(\Delta_a)$. (The definition is external in the sense that it only gives values of Df for standard values of a .)

We may in turn apply Leibniz' Principle to condition (ii) of 2.2 and the extension of the function $x \mapsto Df_x$ and a fixed standard $\varepsilon > 0$ to see that “there exists a $\delta \in {}^*\mathbb{R}^+$ such that whenever $|x - y| < \delta$, then $|(f(y) - f(x))/(y - x) - Df_x| < \varepsilon$ ”. If we select $x \approx a \in {}^\sigma\mathbb{R}$ and $\varepsilon \approx 0$ and also apply condition (ii) we may conclude that $Df_x \approx Df_a$. (Notice that this proves (ii), implies (i).)

2.3. THEOREM. *Let g be an internal real-valued function and $a \in {}^\sigma\mathbb{R}$. The following are equivalent:*

- (i) $g(x) \approx g(a)$ whenever $x \approx a$.
- (ii) *The function g is defined on a standard neighborhood of a and for every $\varepsilon \in {}^\sigma\mathbb{R}^+$ there is a $\delta \in {}^\sigma\mathbb{R}^+$ such that whenever $|x - a| < \delta$, then $|g(x) - g(a)| < \varepsilon$.*

Robinson calls these equivalent conditions *S-continuity* at a .

Theorem 2.3 shows that Df is epsilon-delta continuous at each standard real number, letting $g = {}^*Df = Df$, by the convention not to put $*$'s on functions, and applying Leibniz' Principle to pull the condition back to the standard model, that is, if $\varepsilon \in \mathbb{R}^+$, then

$$\{\delta \in \mathbb{R}^+ : \text{whenever } |x - a| < \delta, \text{ then } |Df_x - Df_a| < \varepsilon\}$$

is nonempty.

Modulo Theorems 2.2 and 2.3 we have shown (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii). Condition (iii) implies (i) since by continuity and Theorem 2.3, $Df_y \approx Df_a$ whenever $y \approx a$. If (i) fails, then

$$\frac{1}{\delta z} [f(x + \delta z) - f(x)] = Df_x + \theta \quad \text{where } \theta \neq 0.$$

By the $*$ -transform of the mean value theorem there is a y between x and $x + \delta z$ where $Df_y = Df_x + \theta$ and either $Df_y \neq Df_a$ or $Df_x \neq Df_a$.

The proofs of Theorems 2.2 and 2.3 share one common feature — they push an infinitesimal condition out to a finite amount. A general formulation of the continuity principle (which we facetiously refer to as Cauchy's) is as follows. We enlarge $L(\in)$ by adding the full "diagram" of ${}^*\mathcal{L}$, that is, a formal constant for each internal set. We extend I' to include these added constants.

2.4. CAUCHY'S PRINCIPLE. *If $P(x)$ is a bounded internal formal property of the free variable x and if $I'\{P(\eta)\}$ holds for every infinitesimal η , then $I'\{P(x)\}$ holds for all x smaller than some standard δ , $|x| < \delta$.*

This was even generalized to topological spaces by Luxemburg, see STROYAN [1976].

PROOF. As we showed in the first section, the infinitesimals o are an external set. The set

$$\{\delta \in {}^*\mathbb{R} : \forall x [|x| < \delta \Rightarrow I'\{P(x)\}]\}$$

is internal and by hypothesis contains all the infinitesimals, so it contains a noninfinitesimal δ . $\square$

PROOF OF THEOREM 2.2. (i) implies (ii): Let $\varepsilon \in {}^\sigma\mathbb{R}^+$ be given. The following set is standard since its description involves only standard constants:

$$\left\{ \delta \in {}^*\mathbb{R}: \text{whenever } |x - a| < \delta, \right. \\ \left. f(x) \text{ is defined and } \left| \frac{f(x) - f(a)}{x - a} - b \right| < \varepsilon \right\}$$

Condition (ii) follows from Cauchy's Principle or alternately from the fact that the above set is nonempty in ${}^*\mathbb{R}$, therefore, by Leibniz' Principle, is nonempty in $\mathbb{R}$ as well.

(ii) implies (i): Let $x \approx a$ in ${}^*\mathbb{R}$. We apply Leibniz' Principle to (ii) for a fixed standard positive ε and standard δ from (ii). Since $|x - a| < \delta$ when δ is standard we know that the infinitesimal difference quotient is within epsilon of b , but epsilon is arbitrary, so (i) holds. $\square$

An Interpretation of Leibniz'

$$\frac{df}{dx}(a)$$

can now be made as the common standard part of *all* the infinitesimal difference quotients

$$\frac{f(a + \delta x) - f(a)}{\delta x}$$

provided they *all* have a common standard part. (We go beyond this below and interpret both df and dx .)

Exercise. Compute dP/dx , for polynomials using the $*$ -binomial theorem on $(a + \delta x)$.

PROOF OF THEOREM 2.3. (i) implies (ii): Since g is internal, the property $P_\varepsilon(\eta) = \text{"whenever } |x - a| < \eta, \text{ then } g(x) \text{ is defined and } |g(x) - g(a)| < \varepsilon\text{"}$ is also internal. Provided ε is standard and positive, Cauchy's Principle applies and gives (ii).

(ii) implies (i): Let $x \approx a$, so $|x - a| < \delta$ whenever δ is standard and positive. Condition (ii) implies then that $|g(x) - g(a)| < \varepsilon$ for any standard positive epsilon, thus $g(x) \approx g(a)$. $\square$

We reiterate the question of the last section: Is the internal function $f(x) = \sin(\pi\Omega x)$ continuous in the *standard* sense?

2.5. DEFINITION. Let $f: [a, b] \rightarrow \mathbb{R}$ be a standard function. To define *Riemann integrals* over $[a, b]$ we partition the interval into a $*$ -finite number of infinitesimal subintervals $a = x_0 < x_1 < \cdots < x_\Omega = b$ with $x_{(k-1)} \approx x_k$ for $1 \leq k \leq \Omega$, internally choose y_k , $x_{(k-1)} \leq y_k \leq x_k$ and compute the $*$ -finite sum:

$$\sum_{k=1}^{\Omega} f(y_k) \cdot [x_k - x_{k-1}]$$

If all these infinitesimal Riemann sums give nearly the same finite answer we call the common standard part *the integral*,

$$\int_a^b f(x) dx.$$

We elaborate on the definition since it is a little complicated. First, the term $*$ -finite means the $*$ -transform of “finite” from the standard model. “Finite” in $\mathcal{X}$ can be written “there is an $n \in \mathbb{N}$ and a bijection from $\{k \in \mathbb{N}: 1 \leq k \leq n\}$ onto P ”, hence a $*$ -finite partition is simply an internal bijection from a set $\{k \in {}^*\mathbb{N}: 1 \leq k \leq \Omega\}$ onto a subset of $[a, b]$. An example is given simply by the equal partition

$$x_k = \frac{k}{\Omega} (b - a) + a, \quad 0 \leq k \leq \Omega.$$

The words “internally choose y_k ” mean $y_{(\cdot)}$ is also an internal function from $1 \leq k \leq \Omega$ into $[a, b]$. Since the function Σ of the standard model is defined for all finite sets of reals, its nonstandard extension is defined for all $*$ -finite sets of hyperreals, thus the $*$ -finite sum exists in ${}^*\mathbb{R}$. While the $*$ -finite sum always exists two $*$ -finite infinitesimal Riemann sums need not be infinitesimally close, for example, let f be the indicator function of the rational numbers, $f(x) = 1$ if x is rational, $f(x) = 0$ if x is irrational, $*$ -irrational y_k ’s give zero sum while $*$ -rational y_k ’s give $(b - a)$ sum, the integral does not exist.

It is fairly easy to see that an internal finite S-continuous function will actually yield a common standard part for all its infinitesimal Riemann sums. For example, if z_k and y_k are two choices of evaluation points:

$$\left| \sum_{k=1}^{\Omega} f(z_k) \Delta x_k - \sum_{k=1}^{\Omega} f(y_k) \cdot \Delta x_k \right| \leq \max_{1 \leq k \leq \Omega} |f(z_k) - f(y_k)| \cdot (b - a)$$

and the internal $*$ -finite maximum is attained with $z_k \approx y_k$ so that $f(z_k) \approx$

$f(y_k)$. Similarly, different partitions have a common refinement by Leibniz' Principle applied to the statement "finite partitions have a common refinement". The sums are close on the common refinement and each refined sum nearly agrees with the old one. In particular *this shows that continuous standard functions are Riemann integrable and for such functions any infinitesimal Riemann sum can be used to evaluate $\int_a^b f(x)dx = \text{st}(\sum_{k=1}^n f(y_k)\Delta x_k)$* . (Well, it does not show the "epsilon-delta" version of Riemann integrable, but our definition is equivalent and perhaps Riemann would not have objected to infinitesimals.)

2.6. THE FUNDAMENTAL THEOREM OF CALCULUS. (i) *Let $f: [a, b] \rightarrow \mathbb{R}$ be a continuous standard function and let $F(x) = \int_a^x f(t)dt$, then $(dF/dx)(x) = f(x)$, $a \leq x \leq b$.*

(ii) *Let $F(x)$ be a uniformly differentiable function in a neighborhood of $[a, b]$, then $\int_a^b (dF/dx)(x)dx = F(b) - F(a)$.*

PROOF. By Leibniz' Principle,

$$\delta z \cdot \min_{x \leq t \leq x + \delta z} [f(t)] \leq \int_x^{x + \delta z} f(t)dt \leq \delta z \cdot \max_{x \leq t \leq x + \delta z} [f(t)],$$

and when $\delta z \approx 0$, $\min f(t) \approx f(x) \approx \max f(t)$, so

$$\frac{dF}{dx}(x) = \text{st} \left(\frac{F(x + \delta z) - F(x)}{\delta z} \right)$$

no matter which infinitesimal we choose. This proves (i).

($\approx$ Cauchy): Let $\{x_k : 0 \leq k \leq \Omega\}$ be an infinitesimal partition. By condition (i) of 2.2,

$$\frac{dF}{dx}(x_k) = \frac{F(x_k) - F(x_{k-1})}{x_k - x_{k-1}} + \eta_k$$

with $\eta_k \approx 0$ for $1 \leq k \leq \Omega$. Hence

$$\sum_{k=1}^{\Omega} \frac{dF}{dx}(x_k) \Delta x_k = \sum_{k=1}^{\Omega} [F(x_k) - F(x_{k-1})] + \sum_{k=1}^{\Omega} \eta_k \Delta x_k$$

and

$$\left| \sum_{k=1}^{\Omega} \eta_k \Delta x_k \right| \leq \max(|\eta_k|) \cdot \sum_{k=1}^{\Omega} \Delta x_k = |\eta_m| \cdot (b - a) \approx 0$$

while

$$\sum_{k=1}^{\Omega} [F(x_k) - F(x_{k-1})] = F(b) - F(a)$$

by transfer of the formula for telescoping sums. This proves (ii). $\square$

We need to cast uniform differentiability in a “several variable” setting (a Banach manifold is really no harder) Let $\mathbb{M} \subseteq \mathbb{R}^n$ be a subset of n -space for some fixed finite n . The metric on $\mathbb{R}^n$ has an extension to ${}^*\mathbb{R}^n$,

$$|X - Y| = \left(\sum_{j=1}^n (x^j - y^j)^2 \right)^{\frac{1}{2}}$$

and we say that *the vector* $X = (x^1, \dots, x^n)$ *is infinitesimally close to the vector* $Y = (y^1, \dots, y^n)$ *when*

$$|X - Y| \approx 0 \quad \text{in } {}^*\mathbb{R}.$$

This is easily seen to be equivalent to $x^j \approx y^j$, $1 \leq j \leq n$. We also might say X is “infinitely near” Y or “nearly equal to” Y . A vector B is “near-standard” if there is a standard vector A such that $B \approx A$. *The vector* x *is finite when* $|X|$ *is finite in* ${}^*\mathbb{R}$. The *standard part* of a finite vector X is the standard vector $\text{st}(X) = (\text{st}(x^1), \text{st}(x^2), \dots, \text{st}(x^n))$.

We include a few results to indicate how topology of subsets of $\mathbb{R}^n$ can be treated with infinitesimals. Instead of dealing with the monad of a standard point, that is, all $X \in {}^*\mathbb{R}^n$ with $X \approx A$, we deal with the relative monad, all $X \in {}^*\mathbb{M}$ with $X \approx A$.

2.7. THEOREM. *A standard subset* $U \subseteq \mathbb{M}$ *is a topological* $\mathbb{M}$ -*neighborhood of* $A \in U$ *if and only if whenever* $X \approx A$, $X \in {}^*\mathbb{M}$, *then* $X \in {}^*U$, *that is, provided* *U *contains the relative-* ${}^*\mathbb{M}$ -*monad of* A .

PROOF. Apply Cauchy’s Principle to the statement

$$“{}^*U \text{ contains the internal set } B(\eta) \cap {}^*\mathbb{M}”$$

where $B(\eta) = \{X \in {}^*\mathbb{R}^n : |X - A| < \eta\}$. Then apply Leibniz’ Principle to the standard δ obtained from Cauchy’s Principle, so

$$“U \text{ contains } B(\delta) \cap \mathbb{M}”, \quad \text{without } {}^*\text{'s}.$$

The converse is immediate from Leibniz’ Principle. $\square$

2.8. THEOREM. *The standard set* $U \subseteq \mathbb{M}$ *is* $\mathbb{M}$ -*closed if and only if whenever* $u \in {}^*U$ *is infinitesimally close to a standard* $m \in {}^\sigma\mathbb{M}$, *then* $m \in {}^\sigma U$. *More specifically, a sequence* $\{X_n\}$ *converges to* A *if and only if* $X_n \approx A$ *for infinite* $\Omega \in {}^*\mathbb{M}_\infty$.

For a proof of Theorem 2.8 or 2.9 see ROBINSON [1966] or STROYAN [1976].

2.9. THEOREM. *A standard set $U \subseteq \mathbb{M}$ is $\mathbb{M}$ -compact if and only if every point $X \in {}^*U$ is near a standard $u \in {}^\sigma U$.*

For example, the open unit interval $(0, 1)$ is *not* compact because ${}^*(0, 1) = \{x \in {}^*\mathbb{R} : 0 < x < 1\}$ contains infinitesimals $\varepsilon \approx 0$, but does not contain 0 itself. The natural numbers are not compact because ${}^*\mathbb{N}$ contains an infinite integer Ω , not near any standard point.

We denote the space of linear maps from $\mathbb{R}^m$ to $\mathbb{R}^n$ by $\text{Lin}(\mathbb{R}^m, \mathbb{R}^n)$. An *internal linear map* is an element of ${}^*\text{Lin}(\mathbb{R}^m, \mathbb{R}^n)$. A finite internal linear map is one which has finite sup norm or equivalently finite scalars in the matrices representing it with respect to standard bases or equivalently one which maps finite vectors to finite vectors.

2.10. THEOREM. *Let $f : U \rightarrow \mathbb{R}^n$ be a standard function defined on $U \subseteq \mathbb{R}^m$. The following are equivalent:*

(i) *There is a standard map $Df : U \rightarrow \text{Lin}(\mathbb{R}^m, \mathbb{R}^n)$ such that whenever x is near a standard point of ${}^\sigma U$, and whenever δz is infinitesimal in ${}^*\mathbb{R}^m$,*

$$f(x + \delta z) - f(x) = Df_x(\delta z) + |\delta z| \cdot \eta$$

for some infinitesimal $\eta \in {}^\mathbb{R}^n$.*

(ii) *For each standard $a \in {}^\sigma U$, there is a finite internal linear map L_a such that whenever $x \approx y \approx a$,*

$$f(y) - f(x) = L_a(y - x) + |y - x| \cdot \eta$$

for some infinitesimal $\eta \in {}^\mathbb{R}^n$.*

(iii) *U is open and f is continuously differentiable on U .*

PROOF. Modify the proof of Theorem 2.1. $\square$

Higher order derivatives are given infinitesimally by the following uniform conditions.

2.11. TAYLOR'S SMALL OH FORMULA. *Let $f : U \rightarrow \mathbb{R}^n$ be a standard map on $U \subseteq \mathbb{R}^m$. The following are equivalent:*

(i) *There exist standard maps $L^h : U \rightarrow \text{S Lin}^h(\mathbb{R}^m; \mathbb{R}^n)$, the symmetric h -linear maps from $\mathbb{R}^m$ to $\mathbb{R}^n$ such that whenever x is near a standard point in *U and δz is infinitesimal in ${}^*\mathbb{R}^m$,*

$$f(x + \delta z) = \sum_{h=0}^k \frac{1}{h!} L_x^h(\delta z)^{(h)} + |\delta z|^k \cdot \eta$$

for some η infinitesimal in ${}^\mathbb{R}^n$.*

(ii) U is open and $f \in C^k(U; \mathbb{F})$.

The maps L^h are h -th-order derivatives of f , $D^h f$.

PROOF. See STROYAN [1976], §5.7.9.

3. Continuous curvature and differentials

Article 3 in GAUSS [1827], the magnificent *Disquisitiones generales circa superficies curvas*, begins as follows.

“A curved surface is said to possess continuous curvature at one of its points A , if the directions of all straight lines drawn from A to points of the surface at an infinitely small distance from A are deflected infinitely little from one and the same plane passing through A . This plane is said to *touch* the surface at the point A ”.

This motivates the following definition.

3.1. DEFINITION. A subset $M \subseteq \mathbb{R}^n$ is an m -manifold with continuous curvature provided that there is a standard map τ from the points of M into the affine m -dimensional planes of $\mathbb{R}^n$ satisfying:

- (i) If $A \in M$, then τ_A contains A .
- (ii) For each near-standard $A \in {}^*M$, the orthogonal projection from *M to τ_A maps the set of $B \in {}^*M$ with $B \approx A$ onto the set of $b \in \tau_A$ satisfying $b \approx A$.
- (iii) For each near-standard $A \in {}^*M$ and $B \in {}^*M$ with $B \approx A$, if $B - A = t + n$ where t lies in τ_A and n is normal to τ_A , then $|n|/|B - A| \approx 0$.

Condition (i) says a preferred m -plane meets M at A . Condition (ii) says M infinitesimally has dimension at least m , and (iii) says the deflection angle from the tangential component is infinitesimal. It is important that we treat all the near-standard points of *M alike, otherwise we only get “differentiable” and not “ C^1 ”. Notice that (iii) forbids improperly embedded manifolds as well as kinks (see Fig. 5).

3.2. THEOREM. If M is an m -manifold in $\mathbb{R}^n$ with continuous curvature in the sense of Gauss, then M is a C^1 - m -manifold in the sense of Weyl with charts given by local projection onto the tangent planes.

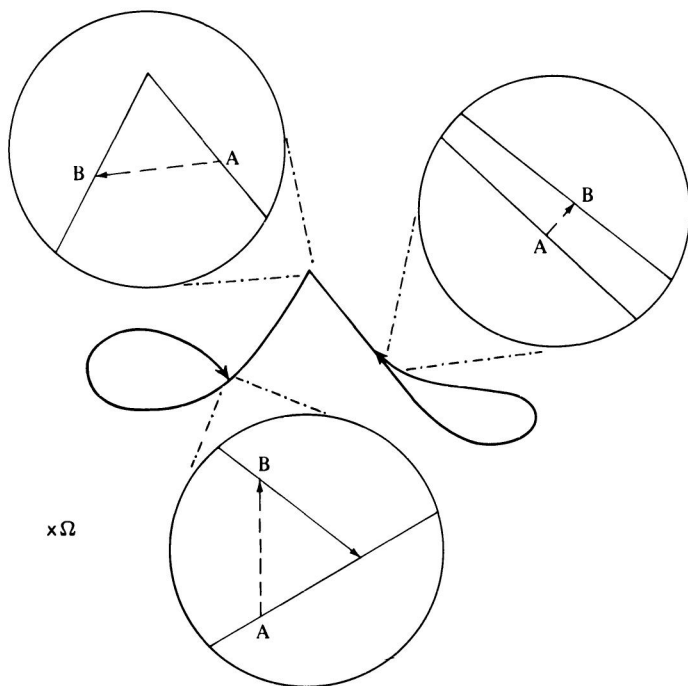


Fig. 5.

A “ C^1 -manifold in the sense of Weyl” means the conventional abstract manifold definition, M is covered by an *atlas* of charts where each *chart* is a homeomorphism φ from a subset of M onto an m -dimensional ball. The charts satisfy the *overlap condition* that when $\varphi \circ \psi^{-1}$ is defined for two charts, it is a C^1 map from $\mathbb{R}^m$ to $\mathbb{R}^m$.

PROOF. First we show that *when A and B are near-standard on *M , with $A \approx B$, then $\mathbb{T}_A$ is nearly parallel to $\mathbb{T}_B$* (or equivalently since $A \approx B$, the tangent planes have the same standard part, that is, there is a standard plane P so $\text{st}(\mathbb{T}_A) = \text{st}(\mathbb{T}_B) = P$). Let $\delta = |B - A| \neq 0$. The unit vectors, $\text{st}((B - A)/\delta) = -\text{st}((A - B)/\delta)$ lie in the intersection $\text{st}(\mathbb{T}_A) \cap \text{st}(\mathbb{T}_B)$. By (iii) we have

$$\frac{B - A}{\delta} = \frac{n_A}{\delta} + \frac{t_A}{\delta} \approx \frac{t_A}{\delta},$$

normal + tangent in $\mathbb{T}_A$, and

$$\frac{A - B}{\delta} = \frac{n_B}{\delta} + \frac{t_B}{\delta} \approx \frac{t_B}{\delta},$$

normal + tangent in $\mathbb{T}_B$, hence, $t_A/\delta \cdot t_B/\delta \approx -1$ and the projection of one on the other has the same standard part. It simplifies our notation to write $B - A \approx^\delta t_A$ for $(B - A)/\delta \approx t_A/\delta$, etc. By the onto assumption (ii) there are points C, D in ${}^*\mathbb{M}$ such that $\delta = |C - A| = |D - B|$ and the angle between $C - A$ and $D - B$ is the angle of $\mathbb{T}_A$ with $\mathbb{T}_B$. Also, by (iii) $C - A \approx^\delta t_C$ in $\mathbb{T}_A$ and $D - B \approx^\delta t_D$ in $\mathbb{T}_B$. Now, $C - A + A - B \approx^\delta t_C + t_B \approx^\delta t_C - t_A \approx^\delta C - B$ so that $\mathbb{T}_A$ is nearly parallel to $\mathbb{T}_B$, since the angle-forming vectors lie δ -nearly in both $\mathbb{T}_A$ and $\mathbb{T}_B$:

$$0 \approx^{\delta^2} (C - A) \cdot (D - B).$$

Second, the orthogonal projection from ${}^*\mathbb{M}$ onto $\mathbb{T}_A$ is one-to-one on the infinitesimal neighborhood of a near-standard vector on ${}^*\mathbb{M}$. Suppose $B - A = T + M$ and $C - A = T + N$ where M and N are normal to $\mathbb{T}_A$. $C - B = C - A + A - B = N - M$, yet lies nearly in $\mathbb{T}_B$ by (iii) and nearly in $\mathbb{T}_A$ since $\mathbb{T}_A$ is nearly parallel to $\mathbb{T}_B$. Hence $M = N$.

Consider the property $P(\eta)$: "orthogonal projection from the set of B on ${}^*\mathbb{M}$ such that $|B - A| < \eta$ is a bijection onto its image in $\mathbb{T}_A$ ". By the above remarks, $P(\eta)$ holds for every positive infinitesimal. Cauchy's Principle shows that projection is a local bijection.

Take two near-standard points A, B on ${}^*\mathbb{M}$ with projections P_A, P_B which are bijective on neighborhoods overlapping at the near-standard point C . The maps P_A and P_B defined by neglecting the normal component of the displacement vectors are definable everywhere in ${}^*\mathbb{R}^n$ and in particular, on $\mathbb{T}_C$. We consider the "reflection" of $\mathbb{T}_A$ on $\mathbb{T}_B$ thru $\mathbb{T}_C$ as shown schematically in Fig. 6, $\psi = P_B \circ (P_A^{-1} \upharpoonright \mathbb{T}_C)$.

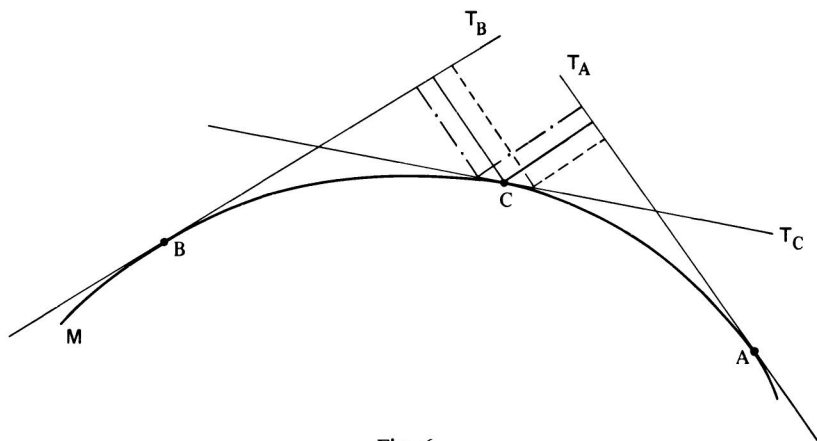


Fig. 6.

This is a linear map in the displacement from $P_A(C)$ to the displacement from $P_B(C)$. The actual overlap map is $\varphi = P_B \circ P_A^{-1}$, that is, project down to $\mathbb{M}$ from $\mathbb{T}_A$ and back to $\mathbb{T}_B$, as shown schematically in Fig. 7.

Without essential restriction we may assume that $\mathbb{T}_A$, $\mathbb{T}_B$, and $\mathbb{T}_C$ all meet at acute angles.

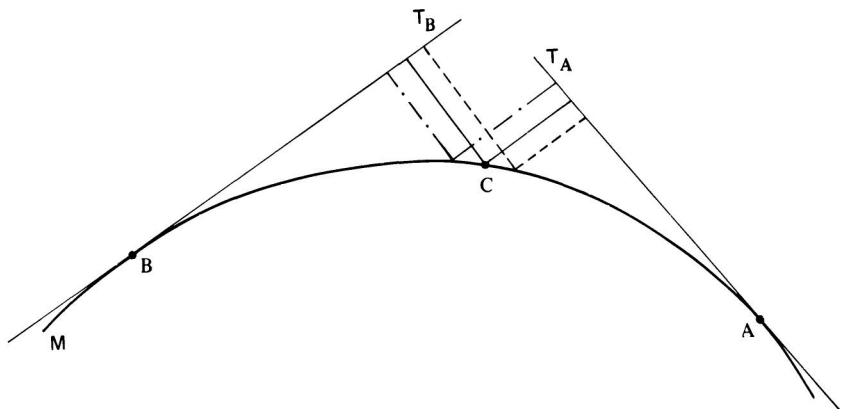


Fig. 7.

We take $c = P_A(C)$ and let $x \approx c$ on $\mathbb{T}_A$. Also, let $X = P_A^{-1}(x)$. P_A is continuous so that $X \approx C$ and we may apply Gauss' condition to see that $\varphi(x)$ and $\psi(x)$ differ by an infinitesimal multiple of $|X - C|$. This only requires a little trigonometry comparing the difference between reflection from $\mathbb{T}_C$ and $\mathbb{M}$ which we leave to the reader. This is a proof of the uniform differentiability of φ at C .

Applying Theorem 2.10 we see that the overlap maps are C^1 . $\square$

Let A be near-standard on ${}^*\mathbb{M}$ and $0 < \delta \approx 0$. We shall write

$$E \approx^\delta F \quad \text{provided} \quad \frac{|E - F|}{\delta} \text{ is infinitesimal}$$

and say E is " $\approx^\delta$ -nearly equal to" F or E differs " δ -infinitesimally" from F . Gauss' condition means that the set

$$\delta\mathbb{M} = \left\{ B \in {}^*\mathbb{M}: \frac{|B - A|}{\delta} \text{ is finite} \right\}$$

is $\approx^\delta$ -nearly on $\mathcal{O}$ -vector space with A as the zero. More specifically, linear combinations in ${}^*\mathbb{R}^n$ of displacement vectors with finite scalars project back into $\delta\mathbb{M}_A$ with at most an error which is infinitesimal when divided by

δ . Another way to view this is that $\delta\mathbb{M}_A$ only differs δ -infinitesimally from its projection on $\mathbb{T}_A$ and that *is* a vector space. This provides the link between infinitesimals on a fixed scale and differential forms. If ζ is a standard C^1 -covector valued map on $\mathbb{M}$, then $\delta \cdot \zeta_A + A$ can be thought of as nearly in $\delta\mathbb{M}_A$, inverting the projection from $\mathbb{T}_A$ (and using the ambient inner product for a vector-covector isomorphism). On the other hand, if $x : {}^*\mathbb{M} \rightarrow {}^*\mathbb{R}^n$ is an internal finite map such $\delta \cdot x(A) \in \delta\mathbb{M}_A$ and x has a finite linear approximation in the sense of 2.10, *we may interpret*

$$dx$$

as the $\approx^\delta$ -equivalence class of the map. The usage of infinitesimals in local geometry usually does not require a function, but rather only a single $\approx^\delta$ -class of perturbations. Picard's existence theorem for differential equations would let us localize such an infinitesimal condition. We regret lacking the space to do this in greater detail, the reader can decide which way Gauss intended.

The exterior algebra of the space $\delta\mathbb{M}_A$ can now be constructed identifying near-parallelograms of A, B, C and A, D, E where $|B - A|, |C - A|, |D - A|$ and $|E - A|$ are all δ -finite provided $\{B - A, C - A\}$ and $\{D - A, E - A\}$ span the same subspace of $\mathbb{T}_A$ *and have nearly the same area after division by δ^2* (and so on, up to m -forms). We call such a pair a δ -area element when the area divided by δ^2 is noninfinitesimal.

We may interpret the δ^2 -equivalence class of an internal assignment of such δ -area elements,

$$d^2\Sigma$$

as a 2-form (and so on, up to m -forms. A complete local account of forms is given in STROYAN [1976], Ch. 5).

4. Kissing curves

We shall begin our study of curves in $\mathbb{R}^3$ with a construction of the osculating circle, the circle which exactly kisses a curve at a point on the curve. We rely on the Gaussian Definition 3.1 of a curve Γ where $m = 1$. We may parametrize the curve locally with the length u along a tangent line (3.2) and unit tangents are approximated by

$$T_A \approx \frac{B - A}{|B - A|}$$

whenever $B \approx A$ on Γ . ROBINSON [1966] gives an infinitesimal account of arc length when Γ is given by a regular smooth parametric function $X(t)$. In that case,

$$T_A = \frac{\frac{dX}{dt}}{\frac{ds}{dt}} = \frac{\text{st} \left(\frac{X(t + \delta t) - X(t)}{\delta t} \right)}{\text{st} \left(\frac{|X(t + \delta t) - X(t)|}{\delta t} \right)}$$

when A is standard, $A = X(t)$, $B = X(t + \delta t) \approx A$. With length along the tangent line as parameter $|X(u) - A| = (u)(1 + \varepsilon)$, by (3.1), so

$$\frac{du}{ds}(A) = 1 \quad \text{and} \quad \frac{dX}{du}(A) = \frac{dX}{ds}(A) = T_A.$$

Now consider the normal displacement n of a point infinitesimally far from A in the case where X is twice continuously differentiable, $n = [X(\delta) - A - \delta T_A]$. To begin with, by Taylor's formula $n = \frac{1}{2} \delta^2 (d^2 X/du^2)(A) + \delta^2 \cdot \eta$ with $\eta \approx 0$, and $(d/du)(dX/du)(A) = dT/ds(A)$. We let $\kappa_A = dT/ds(A)$ assume $\kappa_A \neq 0$, so T_A and n determine a plane $\mathbb{P}$ thru A . We let D be the intersection of the line parallel to n thru A and the normal bisector of AB in the plane $\mathbb{P}$, $B = X(\delta)$.

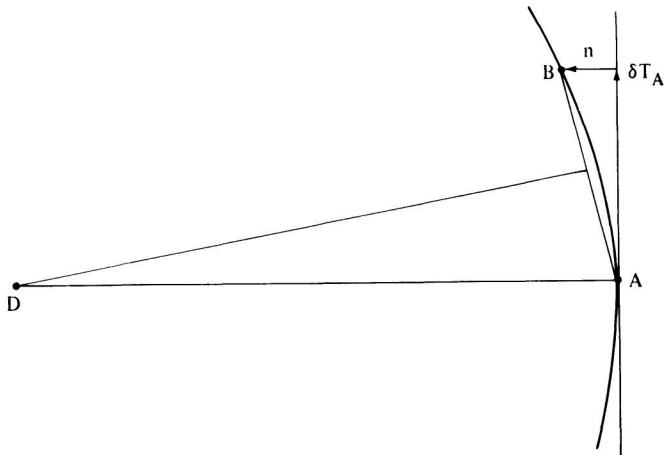


Fig. 8.

The triangles of Fig. 8 are similar so that

$$\frac{|D - A|}{|B - A|} = \frac{|B - A|}{2|n|} \quad \text{and} \quad |B - A| = \delta(1 + \varepsilon),$$

so

$$D - A = (1 + \varepsilon)^2 \frac{\delta^2}{2|n|} \cdot \frac{n}{|n|} \approx \frac{1}{\left| \frac{dT}{ds}(A) \right|} \cdot \frac{\frac{dT}{ds}(A)}{\left| \frac{dT}{ds}(A) \right|}$$

Moreover, the circle thru A and B with center D has a circular standard part, the standard circle tangent to the curve with radius $1/|\kappa_A|$, pointing in the direction of κ_A . This clearly does not depend on the choice of δ , in fact, C_A is the standard part of the infinitesimal tube

$$\{Y: |Y - D| \cdot |\kappa_A| \approx 1\}.$$

The circle thru any three points F, B, E near A on the curve lies inside this tube as we now demonstrate. Suppose B lies between F and E and $|E - B| > |F - B|$. By Taylor's formula,

$$E - B = \varepsilon T_B + \frac{\varepsilon^2}{2} \kappa_B + \varepsilon^2 \eta, \quad \frac{\varepsilon}{|E - B|} \approx 1, \quad \eta \approx 0,$$

and

$$B - F = \varphi T_B + \frac{\varphi^2}{2} \kappa_B + \varphi^2 \zeta, \quad \frac{\varphi}{|F - B|} \approx 1, \quad \zeta \approx 0,$$

so

$$\frac{1}{\varepsilon} \left[\frac{B - F}{|B - F|} \times \frac{E - B}{|E - B|} \right] \approx \frac{(1 + \varphi/\varepsilon)}{2} (T_B \times \kappa_B) \approx \frac{(1 + \varphi/\varepsilon)}{2} (T_A \times \kappa_A).$$

This proves that the plane of FBE is nearly the osculating plane. By (3.1) the angle between $B-F$ and $E-B$ is infinitesimal, thus the normal bisection plane of EB is nearly perpendicular to $T_B \approx T_A$ and it suffices to show that the radius r of the circle through F, B , and E is nearly $1/|\kappa_A|$. By simple trigonometry and the fact that the angle between $B-F$ and $E-B$ is infinitesimal we see that

$$\frac{2r}{|E - F|} : \frac{|E - B|}{\left| (E - B) + \frac{\varepsilon}{\varphi} (F - B) \right|} \approx 1$$

and using the Taylor expansions above, $r \approx 1/|\kappa_B| \approx 1/|\kappa_A|$. (The reader may wish to supply the details. It is quite easy to show that the circle thru three equally spaced points is nearly C_A .)

So far we have shown: $(dT/ds)(A) = \kappa_A$, the curvature vector, is normal to the unit tangent T_A . We let $N_A = \kappa_A/|\kappa_A|$ denote the principal normal.

$(1/|\kappa_A|)N_A$ points from A to the center of the osculating circle. The standard part of the circle thru any three points infinitesimally near A equals the osculating circle.

The curvature vector κ can change in two ways as we move along the curve. First, by increasing or decreasing in magnitude and second by moving from the plane of the starting tangent and curvature vectors. Taking four equally spaced infinitesimally nearby points $A = X(0)$, $C = X(\delta)$, $D = X(2\delta)$, $E = X(3\delta)$, assuming $X(s) \in C^3$ and using Taylor's formula, we find that the change in curvature from C to D is $[(E - D) - (D - C)] - [(D - C) - (C - A)] = \delta^3 \cdot d^3 X/ds^3 + \delta^3 \cdot \eta$ (see Fig. 9).

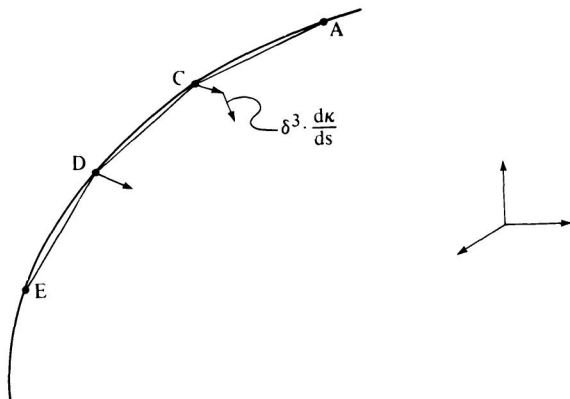


Fig. 9.

The reader should notice that it greatly simplifies the notation in the calculation if one writes $\delta^3 \cdot o$ to mean “ δ^3 times some infinitesimal vector”, so

$$X(2\delta) = A + 2\delta T + \frac{(2\delta)^2}{2} \kappa + \frac{(2\delta)^3}{6} \cdot \frac{d\kappa}{ds} + \delta^3 \cdot o,$$

$$X(\delta) = A + \delta \cdot T + \frac{\delta^2}{2} \kappa + \frac{\delta^3}{6} \frac{d\kappa}{ds} + \delta^3 \cdot o,$$

etc. This is the infinitesimal form of the Landau “small oh” calculus and our motivation for the name of the infinitesimals.

The change in the unit normal from C to D on (4.2) is

$$\frac{[(E - D) - (D - C)]}{\delta^2 |\kappa|} - \frac{[(D - C) - (C - A)]}{\delta^2 |\kappa|} = \delta \cdot \frac{1}{|\kappa|} \frac{d\kappa}{ds} + \delta \cdot o.$$

We complete our standard moving frame of orthogonal unit vectors T , $N = \kappa / |\kappa|$ with the binormal $B = T \times N$. The change in the unit normal above lies nearly in the plane of T and B , it is nearly normal to N , so we decompose it into (T, B) -coordinates $0 = d/ds(\kappa \cdot T) = (d\kappa/ds) \cdot T + |\kappa|^2$,

so $(d\kappa/ds) \cdot T = -|\kappa|^2$. We denote the remaining part by $\tau = |\tau|B$, for torsion.

$T(s + \delta) = T(s) + \delta|\kappa|N + \delta o$, by Taylor's formula. $N(s + \delta) = N(s) - \delta|\kappa|T + \delta|\tau|B + \delta o$, by the calculations above for the change in the normal and the T -component. $B(s + \delta) = B(s) - \delta|\tau|N + \delta o$, simply by a "small oh" calculation with the above formulas in $B(s + \delta) = T(s + \delta) \times N(s + \delta)$. Summarizing, $\text{mod } \approx^\delta$ we have the Serret-Frenet formulas for the moving frame:

$$\begin{aligned}dT &= |\kappa|Nds, \\dN &= -|\kappa|Tds + |\tau|Bds, \\dB &= -|\tau|Nds.\end{aligned}$$

The sphere thru the four points A, C, D, E contains all this information geometrically. Its standard part is called the *osculating sphere*. The plane of T and N cuts this sphere in the previously computed osculating circle. The center of the sphere lies above the center of the osculating circle along the vector

$$\frac{1}{|\tau|} \frac{d\left(\frac{1}{|\kappa|}\right)}{ds} B,$$

where the two coefficients incorporate the twist in the plane of T, N and the straightening of the radius of curvature, respectively. We leave the calculation to the reader. Note:

$$\frac{d^3X}{ds^3} = -|\kappa|^2 T + \frac{d|\kappa|}{ds} N + |\kappa||\tau|B.$$

The formulas for the moving frame take a simple form if one computes the axis of rotation in moving the frame at C to the frame at D . One obtains

$$dT = R \times T ds, \quad dN = R \times N ds, \quad dB = R \times B ds,$$

where $R = |\tau|T + |\kappa|B$. We also leave this calculation to the reader.

5. Gauss' investigations of surfaces

In this section we give a brief account of the role of infinite and infinitesimal vectors in GAUSS [1827].

Surfaces embedded in E^3 have tangent bundles with simpler descriptions

than abstract manifolds. We gain enough in intuition and technical ease in such a setting that an apology for lack of generality would be unnecessary even if Gauss' results were not as profound as they are.

In his *Abstract* of the *Disquisitiones generales circa superficies curvas*, Gauss states the following. "In researches in which an infinity of directions of straight lines in space is concerned, it is advantageous to represent these directions by means of those points upon a fixed sphere, which are the end points of the radii drawn parallel to the lines. The center and the radius of this auxiliary sphere are here quite arbitrary. The radius may be taken equal to unity. This procedure agrees fundamentally with that which is constantly employed in astronomy, where all directions are referred to a fictitious celestial sphere of infinite radius". Naturally, infinitesimal analysis could rigorously provide us with a celestial sphere of infinite radius which we could use to trace Gauss' investigations. But as Gauss himself points out, we may as well normalize after we map the various things on that sphere anyway.

In *Article 4*, Gauss lets L be a point on the auxiliary sphere corresponding to a unit normal to $\mathbb{T}_A$ and also takes a point infinitesimally near A (δ -infinitely far from A) with coordinates $x + \delta x$, $y + \delta y$, $z + \delta z$ where A has coordinates x , y , z . If L has coordinates X , Y , Z , then Gauss' tangency condition (in Definition 3.1) directly implies

$$(X, Y, Z) \cdot (\delta x, \delta y, \delta z) \approx^{\delta} 0$$

or

$$X dx + Y dy + Z dz = 0,$$

after factorization $\text{mod } \approx^{\delta}$. The remainder of *Article 4* is devoted to deriving the form of this equation, first, when $\mathbb{M}$ is given as a null-set of a function W , $\mathbb{M} = \{x: W(x) = 0\}$, second, when $\mathbb{M}$ is given by two coordinate maps, and third, when z is given as a function of x and y .

In the first case, we take dW for the equivalence class $\text{mod } \approx^{\delta}$ of

$$W(x + \delta x, y + \delta y, z + \delta z) - W(x, y, z) \approx^{\delta} dW.$$

Naturally,

$$dW = Pdx + Qdy + Rdz$$

where

$$P = \frac{\partial W}{\partial x}, \quad Q = \frac{\partial W}{\partial y}, \quad R = \frac{\partial W}{\partial z}$$

by Theorem 2.10, provided W is uniformly differentiable, so

$$P \cos(1)\lambda + Q \cos(2)\lambda + R \cos(3)\lambda \approx^{\delta} 0,$$

since W does not change on $\mathbb{M}$. This is true for each direction λ arising from a (δ -finite) infinitesimal perturbation of A on $\mathbb{M}$ (by the onto assumption), thus we obtain Gauss' formula for the normal coordinates

$$X = \frac{P}{\sqrt{(P^2 + Q^2 + R^2)}}, \quad Y = \frac{Q}{\sqrt{(P^2 + Q^2 + R^2)}}, \quad Z = \frac{R}{\sqrt{(P^2 + Q^2 + R^2)}},$$

or the negative of each.

We leave the account of the infinitesimals in the other forms of the formula to the reader.

In *Article 5*, Gauss discusses the local orientation of the normal vector to the surface. We add the following to that discussion. Nearby tangent planes are nearly parallel, thus the internal statement, "a direction of the normal line at B forms an acute angle to the direction selected for the normal line at A " holds on the infinitesimal neighborhood of A and since that set is external, out to some finite radius around A . On that set, the acute normal at B agrees with the orientation of A 's. In words, *consistent local orientation also follows directly from Gauss' condition of continuous curvature*.

Article 6 introduces the map which is now frequently called the Gauss map, namely, over a consistently oriented portion of $\mathbb{M}$ we send $A \mapsto n(A)$ the unit normal on the auxiliary sphere.

The *integral curvature* of a portion of $\mathbb{M}$ is defined to be the area of its image on the auxiliary sphere. Now we take a standard point A on $\mathbb{M}$ and a δ -area element in the sense of the last section. The ratio of the internal integral curvature of the volume element divided by the area of the volume element (which we can compute as a parallelogram on $\mathbb{T}_A$ with only δ^2 -error) is a finite number whose standard part Gauss calls the *measure of curvature* of $\mathbb{M}$ at A . This exists and is well defined independent of δ and the particular δ -area element by standard results of infinitesimal calculus.

The following is an account of Gauss' *Article 7* with some changes in notation (and perhaps δ -infinitesimal differences). Three (δ -finite) infinitesimally close points on $^*\mathbb{M}$, A, B, C span a parallelogram on $\mathbb{T}_A$ with sides AB and AC whose area in δ^2 -nearly equal to that of the projected image on $^*\mathbb{M}$. This is a δ -area element on $^*\mathbb{M}$ in the cases where $B - A$ and $C - A$ have a finite angle between them and are not δ -infinitesimal. We assume this to be the case and denote it by $d^2\sigma \pmod{\delta^2}$.

The area element $d^2\sigma$ is mapped to a figure on the auxiliary sphere under the Gauss map n , moreover, $n(A + E) \approx^\delta n(A) + Dn_A(E)$, whenever $A + E$ is in $\delta\mathbb{M}_A$, in fact, $n(A + E) = n(A) + Dn_A(E) + |E|\eta_E$ and the error η_E is bounded by the infinitesimal $\max[|\eta_E| : A + E \in d^2\sigma]$.

Thus we replace $n(d^2\sigma)$ by $d^2\Sigma$, the projection on the auxiliary sphere of the parallelogram spanned by $n(A)$, $n(B)$, $n(C)$ on the tangent plane to the sphere at $n(A)$. Again, since the sphere has uniformly continuous curvature, the area (mod δ^2) of $d^2\Sigma$ can be calculated either on the sphere or the tangent plane at $n(A)$.

Now, the measure of curvature

$$k(A) \approx \frac{\text{area}(d^2\Sigma)}{\text{area}(d^2\sigma)}$$

and we could use the familiar cross product formula for the respective areas on the respective tangent planes. Article 7 is a derivation of the formula for k in the case where $\mathbb{M}$ is given in Gauss' third form, $z = f(x, y)$. In this case $\mathbb{T}_A$ is not perpendicular to the xy -plane and thus

$$\frac{\text{area}(d^2\Sigma)}{\text{area}(d^2\sigma)} = \frac{\text{area}(\text{projection of } d^2\Sigma \text{ on } xy\text{-plane})}{\text{area}(\text{projection of } d^2\sigma \text{ on } xy\text{-plane})} \quad (5.1)$$

We denote the coordinates of the xy -projections:

$$\begin{aligned} A: \quad x \quad, \quad y \quad \quad \quad n(A): \quad X \quad, \quad Y \\ B: \quad x + \delta_1 x, \quad y + \delta_1 y \quad \quad n(B): \quad X + \delta_1 X, \quad Y + \delta_1 Y \\ C: \quad x + \delta_2 x, \quad y + \delta_2 y \quad \quad n(C): \quad X + \delta_2 X, \quad Y + \delta_2 Y. \end{aligned}$$

The areas of the parallelograms are then

$$(\delta_1 x)(\delta_2 y) - (\delta_2 x)(\delta_1 y), \quad (\delta_2 X)(\delta_1 Y) - (\delta_2 X)(\delta_1 Y), \quad (5.2)$$

respectively.

X and Y are functions of x and y since $\mathbb{M}$ is given by $z = f(x, y)$ and

$$\delta_1 X = X(B) - X(A) \approx \frac{\partial X}{\partial x} \delta_1 x + \frac{\partial X}{\partial y} \delta_1 y,$$

$$\delta_2 X = X(C) - X(A) \approx \frac{\partial X}{\partial x} \delta_2 x + \frac{\partial X}{\partial y} \delta_2 y,$$

$$\delta_1 Y = Y(B) - Y(A) \approx \frac{\partial Y}{\partial x} \delta_1 x + \frac{\partial Y}{\partial y} \delta_1 y,$$

$$\delta_2 Y = Y(C) - Y(A) \approx \frac{\partial Y}{\partial x} \delta_2 x + \frac{\partial Y}{\partial y} \delta_2 y.$$

Now substitute this into (5.2) and then into (5.1) to obtain

$$k = \frac{\partial X}{\partial x} \cdot \frac{\partial Y}{\partial y} - \frac{\partial X}{\partial y} \cdot \frac{\partial Y}{\partial x}$$

with "equality" rather than only "infinitesimally nearly" since both sides are standard.

The infinitesimal account of the remainder of Article 7 is left to the reader.

In Article 8, Gauss derives the theorem of Euler which says that amongst the curves formed by the intersection of $\mathbb{M}$ and planes containing the normal thru A , those of maximum and minimum curvature are at right angles. He also shows that the product of these maximum and minimum curvatures is the measure of curvature " $k = TV$ ". We paraphrase as follows.

Fix a point A on $\mathbb{M}$ and select a coordinate system with zero at A , the z -axis along the normal to $\mathbb{T}_A$ and x°, y° perpendicular coordinates in $\mathbb{T}_A$. Gauss' tangency condition means that z vanishes to the first order near A . If $\mathbb{M}$ is C^2 , and (x°, y°, z) is a δ -finite vector

$$z = \frac{1}{2} T^\circ (x^\circ)^2 + U^\circ x^\circ y^\circ + \frac{1}{2} V^\circ (y^\circ)^2 + \delta^2 \cdot o.$$

Turning the axes of x and y thru an angle θ with

$$\tan 2\theta = \frac{2U^\circ}{T^\circ - V^\circ}$$

it is easily seen that the new formula for z is

$$z = \frac{1}{2} T x^2 + \frac{1}{2} V y^2 + \delta^2 \cdot o.$$

(I) If the curved surface is cut by the plane normal to $\mathbb{T}_A$ containing the x - and z -axes, the curvature of the resulting curve is T . The sign of T says whether the curve bends above or below $\mathbb{T}_A$.

(II) In like manner V represents the curvature cut by the normal plane thru the y - and z -axes with the same sign convention.

(III) Setting $x = r \cos \varphi$ and $y = r \sin \varphi$, the equation

$$z = \frac{1}{2} (T \cos^2 \varphi + V \sin^2 \varphi) r^2 + r^2 \cdot o,$$

for infinitesimal r , gives the curvature

$$T \cos^2 \varphi + V \sin^2 \varphi$$

to the curve cut on $\mathbb{M}$ by the normal plane thru the z -axis making an angle φ with the x -axis.

(IV) Therefore, whenever $T = V$ all curves cut by normal planes thru the z -axis have the same curvature. When T and V are not equal but have the same sign, one is the maximum and other the minimum of all such normal curvatures. On the other hand, one has the greatest convex

curvature, the other the greatest concave curvature, if T and V have opposite signs.

(V) The measure of curvature at A takes the very simple form

$$k = TV.$$

We see this by computing with $(x, y) = (\delta, 0)$ and $(x, y) = (0, \delta)$ so that the length of $(\delta, 0)$ on the normalized osculating circle is $T\delta$, $(0, \delta)$ normalizes to $V\delta$, so the area of $(d^2\Sigma)$ is $TV\delta^2 \bmod \delta^2$, while the area of $(d^2\sigma)$ is $\delta^2 \bmod \delta^2$. (In terms of Dn ,

$$Dn = \begin{pmatrix} T & 0 \\ 0 & V \end{pmatrix}$$

in (x, y) -coordinates.) This shows Gauss' result for Article 8:

5.1. THEOREM. *The measure of curvature at a point A of a C^2 -surface is the product of the extreme curvatures of curves cut by normal planes thru $n(A)$. These extreme curvatures occur at right angles.*

We believe that this is enough infinitesimal analysis to prepare the reader for Gauss' subsequent uses of infinitesimals — it does leave some fascinating reading to test infinitesimals on.

References*

BEHRENS, M.F.

[1969] Untitled preprint.

[1974a] Analytic sets in $\mathcal{M}(D)$, in: HURD and LOEB [1974].

[1974b] A local inverse function theorem, in: HURD and LOEB [1974].

BERKELEY, G.

[1734] A discourse addressed to an infidel mathematician, in: *The Analyst*, Collected Works, Vol. 4 (London, 1951).

GAUSS, C.F.

[1827] *Disquisitiones generales circa superficies curvas*. [English translation: *General Investigations of Curved Surfaces* (Morehead & Hildebrandt, Princeton, NJ, 1902).]

HURD, A. and P. LOEB, editors

[1974] *Victoria Symposium on Nonstandard Analysis*, Lecture Notes in Mathematics, Vol. 369 (Springer, Berlin).

JENSEN, A.

[1972] A computer oriented version of "non-standard analysis", in: LUXEMBURG and ROBINSON [1972].

* See JOHNSON [1975] for a more complete bibliography.

JOHNSON, D.R.

- [1975] *Bibliography of Nonstandard Analysis* — June, 1975, Lecture Notes in Mathematics Vol. 3, University of Pittsburgh, Pittsburgh, PA.

KEISLER, H.J.

- [1976] *Elementary Calculus: An Approach Using Infinitesimals* (Prindle, Weber & Schmidt), to appear.

LUXEMBURG, W.A.J., editor.

- [1969] *Applications of Model Theory to Algebra, Analysis, and Probability* (Holt, Rinehart, and Winston, New York).

- [1973] What is nonstandard analysis?, *Am. Math. Monthly* **80** (6) pt. II, 38–67.

LUXEMBURG, W.A.J. and A. ROBINSON, editors

- [1972] *Contributions to Non-Standard Analysis* (North-Holland, Amsterdam).

MACHOVER, M. and J. HIRSCHFELD

- [1969] *Lectures on Non-Standard Analysis*, Lecture Notes in Mathematics, Vol. 94 (Springer, Berlin).

NEWMAN, J.R.

- [1956] *The World of Mathematics*, Vol. 1 (Simon and Schuster, New York).

NIJENHUIS, A.

- [1974] Strong derivatives and inverse mappings, *Am. Math. Monthly*, **81** (9), 969–980.

ROBINSON, A.

- [1961] Non-standard analysis, *Proc. Royal Acad. Amsterdam Ser. A*, **64**, 432–440.

- [1966] *Non-Standard Analysis* (North-Holland, Amsterdam; revised ed., 1974).

- [1973] Metamathematical problems, *J. Symbolic Logic*, **38** (3), 500–516.

STROYAN, K.D.

- [1976] (in collaboration with W.A.J. Luxemburg) *Introduction to the Theory of Infinitesimals*, Part 1: Classical infinitesimals, Part 2: Infinitesimals in functional analysis (Academic Press, New York), to appear.

SULLIVAN, K.

- [1974] *The teaching of elementary calculus: An approach using infinitesimals*, Thesis, University of Wisconsin, Madison, WI; summary in: *Am. Math. Monthly*, **83** (5) (1976) 370–375.

Admissible Sets and Infinitary Logic

M. MAKKAI

Contents

1. Introduction	234
2. The Kripke–Platek axiom system	237
3. Examples of admissible sets. The truncation lemma	244
4. Hintikka sets, model existence and Σ -compactness	249
5. Conjunctive game formulas	252
6. Applications of game formulas; completeness	262
7. Σ -saturated structures.	266
8. The covering theorem and Suslin's separation theorem	271
9. The perfect subset theorem	277
References	280

1. Introduction

This chapter has an aim different from that of most of the other chapters of this volume. Whereas those give a comprehensive overview of a well-defined branch of mathematical logic, the present one aims at exposing a remarkable point of contact of several topics in logic each of which has an extensive literature. Those who are more theoretically minded, interested in the explanatory aspects of science, in contrast to the experimentally minded who hunt for new phenomena, would always take time to watch how apparently unrelated or vaguely related topics join in a coherent unity, even though the new results forthcoming from such a state of affairs may not (yet) be spectacular. This chapter is written for such a “theoretically minded” reader.

There are four participants of this affair, viz. (i) admissible sets, (ii) the model theory of $L_{\omega_1\omega}$, (iii) classical descriptive set theory (cf. Chapter C.8), (iv) effective descriptive set theory (hyperarithmetic, Π^1_1 , etc. sets) (cf. also Chapter C.8). These four aspects of our theme will appear quite explicitly in the chapter. There are two further, in this chapter more or less hidden, subjects playing important supporting or motivating roles, viz. set theory and recursion theory. The theory of inductive definability, a topic that recently gained an independent status (cf. Chapter C.7), has important connections to our theme but we will not be able to discuss those.

From the four listed ingredients, the first two will be the “active” ones. Our main theme will be the model theory of admissible fragments of $L_{\omega_1\omega}$ but we will develop it only as far as our results have direct applications to the latter two subjects.

Admissible sets were introduced by KRIPKE [1964] and PLATEK [1966]. Their point of view was primarily that of recursion theory. They generalized ordinary recursion theory of the integers to ordinals smaller than a fixed well-behaved, so called *admissible* ordinal. Originally, admissible ordinals were defined in terms of a recursion theory in the style of the Herbrand–Gödel equation calculus. It was a decisive step to switch from admissible ordinals to *admissible sets*; technically, from the admissible ordinal α to the set L_α of sets constructible before α . As a result, the admissibility condition on α gets translated into an elegant *first-order* axiom system KP, talking about the set-theoretic structure $(L_\alpha, \in \upharpoonright L_\alpha)$.

KP is a very good axiom system. It is simple and also, it has a “self-contained” theory. E.g., one does not need to add the axiom “ $V = L$ ” (that, however, is true in the originally conceived intended models) in order to have most of the desired consequences. It would indeed be a pity if

“ $V = L$ ” were needed since it is by no means a simple or a “natural” axiom.

The connections of admissible sets to effective descriptive set theory (Participant (iv)) were recognized early. The fundamental results that (a) the smallest admissible set beyond the trivial one is $HYP(\omega) = L_{\omega_1^{CK}}$, the set of sets constructible before the Church–Kleene (smallest non-recursive) ordinal ω_1^{CK} and (b) $a \subset \omega$ is hyperarithmetic iff $a \in HYP(\omega)$, were found by Kripke and Platek (cf. 6.5 and 6.6 below).

For a modern treatment of admissible sets, we refer to BARWISE [1975].

The second ingredient is infinitary logic. Infinitary logic essentially started out with the Hanf–Tarski work on incompleteness (HANF [1964]) and it was first systematically investigated by KARP [1964]. From around 1962, the model theory of $L_{\omega_1\omega}$, the tamest infinitary logic, was taken up. For an early account, cf. SCOTT [1965]. A treatment of this theory, in an already mature state, is KEISLER [1971].

The connections between descriptive set theory and infinitary logic were clearly in sight from the beginning. Scott’s isomorphism theorem (SCOTT [1964]) was equivalent to an answer to an old question of Kuratowski. Lopez-Escobar’s generalization of Craig’s interpolation theorem (cf. also below) was a generalization of Suslin’s separation theorem. In general, the connection has the following two aspects. First, infinitary logic replaces classes of points of a space by classes of models. Second, in logic syntactic aspects, only implicit in descriptive set theory, become explicit and give rise to interesting considerations. E.g., Malitz’s preservation theorem (MALITZ [1971]) characterizes sentences of $L_{\omega_1\omega}$ preserved to substructures as those that are logically equivalent to universal ones. Infinite formulas are lurking behind Borel and analytic sets, but one can think of Malitz’s theorem only if formulas have been made explicit. As we see it now, Malitz’s theorem and the Suslin separation theorem have an intimate relationship in a common generalization, cf. MAKKAÏ [1973a].

Vaught has made very important contributions, actually in two opposing directions, to establishing and deepening the connections of descriptive set theory and logic, cf. VAUGHT [1973] and VAUGHT [1974]. One aspect of VAUGHT [1973] will be exposed below in detail. In VAUGHT [1974] a sort of opposite point of view is taken and model theory is being “eliminated” in favor of topological methods — with interesting and surprising success.

The contact (that is the main point of this chapter) between admissible sets and $L_{\omega_1\omega}$ (and $L_{\infty\omega}$) was made by BARWISE [1969]. Barwise introduced *admissible fragments* of $L_{\omega_1\omega}$ (and of $L_{\infty\omega}$), by considering only those formulas that belong to a given admissible set. This step was made in the

spirit of suggestions of Kreisel who had emphasized that pure cardinality considerations (the earlier basis of classification of infinite formulas into the languages $L_{\alpha\beta}$) were too crude to yield any interesting results. The rewards were instant: Barwise's completeness and Σ -compactness theorems (cf. also below) showed that admissible fragments had properties similar to ones of ordinary first-order logic that had long been recognized as basic.

Our point of view of the relationship of admissible sets to logic can be summarized as the phenomenon that can be called the *syntactic completeness* of admissible sets. Let A be a countable admissible set, L_A the fragment $L_{\omega_1\omega} \cap A$. "Syntactic completeness" is exemplified by the following examples. If $\varphi \in L_A$ is logically valid, then not only there is a derivation d of φ in a Gentzen-type, infinitary formal system (by the Completeness Theorem for $L_{\omega_1\omega}$, KARP [1964], LOPEZ-ESCOBAR [1965]) but in fact, d can be chosen in A (Barwise's Completeness Theorem). As a second example, we note that Beth's Definability Theorem is true for single sentences $\varphi(P)$ of $L_{\omega_1\omega}$ (LOPEZ-ESCOBAR [1965], cf. also below). Again, the formula "explicitly defining P " can be chosen in L_A once $\varphi(P)$ belongs to $L(P)_A$. Actually, admissible sets are essentially the optimal solutions to the problem of finding "syntactically complete" fragments of $L_{\omega_1\omega}$.

As another remark, let us note that countable admissible sets will not in general be "semantically complete". E.g., a sentence in L_A might have no model in A , even though it has one. Let us also note that it is easy to construct "syntactically and semantically complete" countable transitive sets (by downward Löwenheim-Skolem arguments, starting from HC, the set of all hereditarily countable sets) but one does not get but a few admissible sets, and not the most interesting ones either, in this way. The basic facts of logic on admissible sets lie therefore somewhat deeper than certain obvious reflection arguments.

The gain of adding admissible sets to the model theoretical-descriptive set-theoretical point of view consists in bridging the gap between non-effective and effective descriptive set theory, a goal that was emphasized already before admissible sets by ADDISON [1962]. To refer to perhaps the main instance of the connection, we will elaborate how (a version of) Kleene's theorem stating that $\text{hyp} = \Delta_1^1$ on the one hand and the Suslin separation theorem on the other become special cases of a single result, cf. Section 8 below.

The chapter is aimed at the model theorist, i.e. someone who has some knowledge and appreciation of the spirit of the model theory of ordinary first-order logic. We have chosen to present those methods of the subject

that are most model theoretical in spirit. In particular, we will feature two recent devices: Vaught's use of *conjunctive game sentences*, and Ressayre's Σ -saturated structures. Let's emphasize that, as a result, we have *not* taken the most direct routes to some of the basic facts (such as the Barwise Completeness Theorem).

The first two sections (after the present one) are largely descriptive and do not contain much in the way of proofs. The main theme is taken up in Section 4; the main line of the model theory is essentially self-contained. Applications to (effective) descriptive set theory are in all of Sections 5 to 9.

2. The Kripke-Platek axiom system

Urelements

Although urelements have not been fashionable for some time, they are coming back into vogue just now, at least in the context of admissible sets; cf. BARWISE [1975]. Axiomatic set theory can be naturally developed with due regard to urelements, without much change of the usual exposition of, e.g., Zermelo-Fraenkel set theory.

Urelements are "points" with no set-theoretical structure, i.e., if u is an urelement, no object whatever is an element of u , $x \notin u$ always. One can describe the Cantorian universe of sets with urelements as follows. Let U be any set the elements of which are called *urelements*. For ordinals α , we define $V_{U,\alpha}$ by $V_{U,0} = U$, $V_{U,\alpha+1} = \mathcal{P}(V_{U,\alpha})$, $V_{U,\lambda} = \bigcup_{\alpha < \lambda} V_{U,\alpha}$ for limit λ , and we put $V_U = \bigcup_{\alpha \in \text{Ord}} V_{U,\alpha}$. V_U is the universe of sets with *support* $\subseteq U$. The usual unramified hierarchy is obtained with $U = \emptyset$. The membership relation $\in_U$ on V_U is naturally defined in such a way that for any $u \in U$, any $x \in V_U$, $x \notin_U u$. Henceforth we write $\in$ for $\in_U$.

In the language of set theory with urelements, we have a predicate U in addition to $\in$ and equality, with the obvious interpretations in V_U when regarded as the *structure* of all sets with support $\subseteq U$. We will use the bold face notation $\in$ and U only for emphasis; usually we will write $\in$ and U even in formulas.

The standard axioms of Zermelo-Fraenkel set theory with the axiom of choice (ZFC) will undergo only obvious changes when formulated as assumptions on V_U . E.g., the axiom of extensionality becomes

$$(\neg Ua \wedge \neg Ub) \rightarrow (\forall x (x \in a \leftrightarrow x \in b) \rightarrow a = b).$$

We will use set-theoretic terminology in connection with V_U ("powerset", "ordinal", etc.) in the expected sense.

We refer to BARWISE [1975] for a discussion why it is reasonable to consider a formulation of set theory, especially *admissible* set theory, using urelements. We can indicate the reason for our interest in urelements as follows. We will consider a special admissible set $HYP_{\mathfrak{M}}$, the *admissible hull* of a structure $\mathfrak{M} = (|\mathfrak{M}|, R_1, \dots, R_t)$. We will have $\mathfrak{M} \in HYP_{\mathfrak{M}}$, in particular, $|\mathfrak{M}| \in HYP_{\mathfrak{M}}$. We want $HYP_{\mathfrak{M}}$ to have model-theoretical significance and for that, we will naturally need that any isomorphism $f: \mathfrak{M} \simeq \mathfrak{N}$ can be extended to an $\in$ -isomorphism of $HYP_{\mathfrak{M}}$ and $HYP_{\mathfrak{N}}$. Clearly, for this we need that elements of $|\mathfrak{M}|$ do not have "set-theoretical individuality" in $HYP_{\mathfrak{M}}$, i.e., that they be urelements in $HYP_{\mathfrak{M}}$.

Apart from $HYP_{\mathfrak{M}}$, there is not much reference to urelements in this chapter.

The introduction of urelements into admissible set theory, $HYP_{\mathfrak{M}}$ and related notions are all due to Barwise, cf. BARWISE [1975]. With minor modifications, this section is based on the same source.

The Kripke–Platek axiom system

2.1. DEFINITION. The collection of Δ_0 *formulas* (of the language $\{\in, U\}$) is the smallest collection Y containing the atomic formulas and closed under the conditions:

- (i) If φ is in Y , so is $\neg\varphi$.
- (ii) If φ and ψ are in Y , so are $\varphi \wedge \psi$ and $\varphi \vee \psi$.
- (iii) If φ is in Y , so are $\forall x \in y (\varphi)$ and $\exists x \in y (\varphi)$.

Note that $\forall x \in y (\varphi)$ means the same as $\forall x [x \in y \rightarrow \varphi]$ and $\exists x \in y (\varphi)$ as $\exists x [x \in y \wedge \varphi]$.

Given a transitive set A (i.e., $x \in A$ and $y \in x$ imply that $y \in A$), we can consider A as a structure for the language $\{\in, U\}$ by interpreting $\in$ by the real $\in$ restricted to A and U by $U \cap A$. Mostly, we will write simply A to denote the structure $(A, \in \upharpoonright A, U \cap A)$.

Now, the main property of Δ_0 formulas is that they are *absolute* for transitive interpretations in the sense of:

2.2. PROPOSITION. *For transitive sets $A, B \subset V_U$, if $A \subset B$, then for any Δ_0 -formula $\varphi(x)$ and any elements a in A , we have $A \models \varphi[a]$ iff $B \models \varphi[a]$ iff $V_U \models \varphi[a]$.*

PROOF. This is an easy induction on the complexity of φ . $\square$

Many elementary concepts of set theory can be formalized with Δ_0 -formulas (e.g., “ f is a function”, “ α is an ordinal” etc.). The significance of this fact is that it doesn’t matter if we evaluate the defining formulas in V_U or in any transitive set containing the object in question.

2.3. DEFINITION. KPU, the Kripke–Platek axiom system with urelements, is the theory over the language $\{\in, U\}$, axiomatized by the universal closures of the following axioms:

Urelements: $U(u) \rightarrow x \notin u$.

Empty set: $\exists x (\neg \dot{U}(x) \wedge \forall y (y \notin x))$.

Extensionality: see above.

Foundation (schema): $\forall x (\forall y \in x \varphi(y) \rightarrow \varphi(x)) \rightarrow \forall x \varphi(x)$ for all formulas $\varphi(x)$.

Pair: $\exists a (x \in a \wedge y \in a)$.

Union: $\exists b \forall y \in a \forall x \in y (x \in b)$.

Δ_0 -*Separation (schema)*: $\exists b \forall x (x \in b \leftrightarrow x \in a \wedge \varphi(x))$ for all Δ_0 -formulas φ (in which b does not occur free).

Δ_0 -*Collection (schema)*: $\forall x \in a \exists y \varphi(x, y) \rightarrow \exists b \forall x \in a \exists y \in b \varphi(x, y)$ for all Δ_0 -formulas φ (in which b does not occur free).

(φ, ψ above may have free variables other than the ones indicated.)

2.4. DEFINITION. An *admissible set* is a transitive set A (in some V_U) that is a model of KPU.

Of course, extensionality and foundation are automatic for transitive sets. These axioms appear in KPU because one considers “non-standard” models of KPU as well, cf. below.

We are going to state some important general derived principles next.

2.5. DEFINITION. A formula of the form $\exists u \varphi(u)$ where φ is Δ_0 , is called a Σ_1 -formula. The class of Σ -formulas is the smallest class Y containing the Δ_0 -formulas and closed under

(a) conjunction and disjunction (condition (ii) of 2.1),

(b) bounded quantification (condition (iii) of 2.1),

(c) existential quantification: if φ is in Y , so is $\exists u \varphi$.

The notion of Π -formula is obtained by replacing $\exists$ by $\forall$ in the last clause. Up to logical equivalence, Π -formulas are exactly the negations of Σ -formulas.

The following is the basic (*upward*) *persistence* property of Σ -formulas.

2.6. PROPOSITION. *Let $A \subset B$ transitive sets $\subset V_U$, $\varphi(x)$ a Σ -formula, $a \in A$. Then $A \models \varphi[a]$ implies $B \models \varphi[a]$ and $V_U \models \varphi[a]$.*

PROOF. This is an easy induction on φ . $\square$

Given a formula φ and a variable w , we write $\varphi^{(w)}$ for the result of replacing each unbounded quantifier in φ by a quantifier bounded by w : $\exists u$ by $\exists u \in w$, $\forall u$ by $\forall u \in w$. w should not occur in φ . If φ is Δ_0 , then $\varphi^{(w)} = \varphi$. It is practically obvious that for Σ -formulas $(\varphi^{(u)} \wedge u \subseteq v) \rightarrow \varphi^{(v)}$ and $\varphi^{(u)} \rightarrow \varphi$ are logically valid.

2.7. PROPOSITION (Σ -reflection principle). *For all Σ -formulas φ the following is a theorem of KPU:*

$$\varphi \leftrightarrow \exists a \varphi(a).$$

In particular, every Σ -formula is equivalent to a Σ_1 -formula in KPU.

PROOF. The proof is by induction on φ . Notice that Δ_0 -collection is a special case of Σ -reflection. Conversely, Δ_0 -collection is used in the proof in the induction step: φ is $\forall u \in v \psi(u)$. $\square$

An easy consequence of 2.7 is Σ -collection, that is, like Δ_0 -collection with φ an arbitrary Σ -formula.

The next definition is fundamental.

2.8. DEFINITION Let A be an admissible set.

(i) A predicate on A is Σ (*light face sigma*) (or, Σ_A) if it is defined by a Σ -formula (in the structure $A = (A, \in \upharpoonright A, \cup \cap A)$, without parameters).

(ii) A predicate $P(x)$ on A is Σ (*bold face sigma*) if it is defined by a Σ -formula with parameters in A , i.e., there is a Σ -formula $\varphi(x, y)$ and fixed elements b in A such that for any a in A , $P(a) \Leftrightarrow A \models \varphi[a, b]$.

(iii) An operation on A is Σ , or Σ , according to its graph.

(iv) A predicate $P \subseteq A^n$ is Δ (or Δ), if both P and its complement $A^n - P$ are Σ (or Σ). ($A^n - P$ being Σ or Σ is the same as P being Π , or Π).

For orientation, at this point the reader should consider the admissible set HF of hereditarily finite sets without urelements and he should see (or at least believe) that the Σ (also, the Σ) predicates on HF (restricted to ω) are exactly the recursively enumerable ones, and hence $\Delta = \Delta =$ recursive. This example is fundamental in so far much we look for on admissible sets

is motivated by a desire to find analogs of facts of ordinary recursion theory, generalized for Σ from r.e., and Δ from recursive.

Emphasizing this analogy, sometimes we say that a is A -finite if $a \in A$, a predicate P is A -recursively enumerable (A -r.e.) if it is Σ_A , A -recursive (A -rec.) if it is Δ_A and an operation F is A -recursive if it is Σ_A .

2.9. PROPOSITION (Δ -separation principle). *For any Σ -formula $\varphi(x)$ and Π -formula $\psi(x)$, perhaps containing other free variables besides x , the following is a theorem of KPU: If for all $x \in a$, $\varphi(x) \leftrightarrow \psi(x)$, then there is b such that $b = \{x \in a : \varphi(x)\}$.*

PROOF. Assume $\forall x \in a (\varphi(x) \leftrightarrow \psi(x))$. Then $\forall x \in a (\varphi(x) \vee \neg \psi(x))$, which is equivalent to a Σ -formula, so by Σ -reflection, there is a c such that

(i) $\forall x \in a [\varphi^{(c)}(x) \vee \neg \psi^{(c)}(x)]$. Let, by Δ_0 -separation, $b = \{x \in a : \varphi^{(c)}(x)\}$. Clearly, every $x \in b$ satisfies $\varphi(x)$. If $x \in a$ and $\varphi(x)$, then $\psi(x)$, so $\psi^{(c)}(x)$ (since ψ is Π). So by (i), $\varphi^{(c)}(x)$. Thus $x \in b$ which shows that b is as desired. $\square$

Notice that the careful formulation of 2.9 has a direct consequence:

2.10. COROLLARY (Δ_A -separation). *For A admissible, for $a \in A$ and for Δ predicate $P(x)$ on A , $\{x \in a : P(x)\}$ is an element of A .*

2.11. COROLLARY (Σ -replacement). *For each Σ -formula $\varphi(x, y)$ the following is a theorem of KPU: If $\forall x \in a \exists! y \varphi(x, y)$, then there is a function f , $\text{dom}(f) = a$, such that $\forall x \in a \varphi(x, f(x))$.*

PROOF. By Σ -collection, there is b such that $\forall x \in a \exists y \in b \varphi(x, y)$. Using Δ -separation, there is an f such that

$$\begin{aligned} f &= \{\langle x, y \rangle \in a \times b : \varphi(x, y)\} \\ &= \{\langle x, y \rangle \in a \times b : \neg \exists z [\varphi(x, z) \wedge y \neq z]\}. \quad \square \end{aligned}$$

2.12. COROLLARY (Σ_A -replacement). *For A admissible, for $a \in A$ and for a Σ_A -function F on A , the restriction $F \upharpoonright a$ is an element of A .*

We have “formal” analogs of the notions in 2.8. A Σ -operation symbol of KPU is an operation symbol F introduced by a new axiom $\forall x \forall y (F(x) = y \leftrightarrow \varphi(x, y))$ with a Σ -formula φ such that $\text{KPU} \models \forall x \exists! y \varphi(x, y)$. A Δ -predicate symbol of KPU is a predicate symbol P introduced by a new axiom $\forall x (Px \leftrightarrow \varphi(x))$ such that φ is Σ and there is a Π -formula $\psi(x)$ with

$KPU \vdash \forall x(\varphi(x) \leftrightarrow \psi(x))$. Of course, the “inessential” extension of KPU by such symbols is a conservative extension of KPU, but more is true. If we allow them to enter atomic formulas and we redefine Δ_0 - and Σ -formulas accordingly, then we obtain formulas that are provably equivalent to Δ - (i.e., both to a Σ - and a Π -formula), respectively, to Σ -formulas in the old sense. Moreover, all the new axioms and derived rules of KPU obtained with the new notions of Δ_0 , Δ and Σ become provable. E.g., for Δ_0 -separation for the new setting, this fact involves the Δ -separation principle (Proposition 2.9) for the old KPU.

These facts are related to the notion of relative admissibility. If S is a finite list of predicates and operations on a transitive set A , then A is said to be admissible *relative to* S if all axioms of KPU, with elements of S appearing in atomic formulas, are true in $\langle A, \in \upharpoonright A, S \rangle$. We have

2.13. THEOREM. *If A is admissible, $\hat{S}$ is a list of Δ_A -predicates and Σ_A -operations on A , then A is admissible relative to $\hat{S}$. Moreover, any notion that is Σ or Δ relative to $\hat{S}$, is already Σ_A , or Δ_A , respectively.*

Finally, we state an absoluteness property of Δ .

2.14. PROPOSITION. *Let $P(x)$ be a Δ -predicate symbol of KPU, $F(x)$ a Σ -operation symbol of KPU, and $A \subseteq B \subset V_U$ admissible sets. Then for a , elements of A , $A \models P[a] \Leftrightarrow B \models P[a] \Leftrightarrow V_U \models P[a]$. Also, A is closed under the operation F^{V_U} (F interpreted in V_U) and in fact, F^{V_U} restricted to A is F^A , F interpreted in A .*

Σ -recursion

Next we state the most important derived principle, Σ -recursion. $TC(x)$ means the transitive closure of the set x , i.e., the smallest transitive set b such that $a \subset b$. For an urelement p , $TC(p) = \emptyset$.

Many transfinite-type inductions can be construed as “inductions on $TC(x)$ ”, i.e., when the induction hypothesis is that the assertion is true for all $y \in TC(x)$. Ordinary transfinite induction falls into this category, as well as what is called induction on infinitary formulas. We will formulate forms of proof and definition by induction “on $TC(x)$ ” that are provable in KPU.

We omit the proof of the existence of a Σ -operation symbol $TC(\cdot)$ in KPU such that it is a theorem of KPU that $TC(a)$ is transitive, $a \subset TC(a)$, and for any transitive b , $a \subset b$ implies $TC(a) \subset b$ (cf. BARWISE [1975]). It is quite easy to show:

2.15. PROPOSITION (TC-induction principle). *For any formula $\varphi(x)$ (with possible other free variables as well), the following is a theorem of KPU: If for each x , $\forall y \in \text{TC}(x) \varphi(y)$ implies $\varphi(x)$, then $\forall x \varphi(x)$.*

2.16. PROPOSITION (Definition by Σ -recursion). *Let G be an $n + 2$ -ary Σ -function symbol, $n \geq 0$. It is possible to define a new Σ -function symbol F so that the following is a theorem of KPU: For all $\mathbf{x} = x_1, \dots, x_n$ and y , $F(\mathbf{x}, y) = G(\mathbf{x}, y, (\lambda z F(\mathbf{x}, z)) \upharpoonright \text{TC}(y))$.*

PROOF. The proof is exactly like the proof of the recursion principle for ZF, cf. 5.6 in Chapter B.1. $\square$

2.17. PROPOSITION (Definition by Σ_A -recursion). *Let A be an admissible set. Let G be an $n + 2$ -ary Σ (respectively, Σ) function on A , $n \geq 0$. There is a Σ (respectively, Σ) function F on A such that F satisfies the identity in 2.16.*

Although 2.17 is not a consequence of 2.16, the latter's proof is easily modified to give 2.17.

2.18. COROLLARY (Definition by TC-recursion of Δ -predicates). *Let P, Q be Δ -predicate symbols of $n + 1$, $n + 2$ arguments, respectively; $n \geq 0$. We can introduce a Δ -predicate symbol R so that the following are provable in KPU:*

$$R(\mathbf{x}, p) \leftrightarrow P(\mathbf{x}, p) \quad \text{for urelements } p,$$

$$R(\mathbf{x}, a) \leftrightarrow Q(\mathbf{x}, a, \{b \in \text{TC}(a) : R(\mathbf{x}, a)\}).$$

There is an obvious variant of 2.18, call it Corollary 2.19, on Δ -predicates on admissible sets.

There are many familiar set-theoretical operations and predicates that can be introduced in KPU as Σ -operations and Δ -predicates, using 2.16 and 2.18. Next we will see important examples of such.

Syntax and semantics of $L_{\infty\omega}$ in KPU

For basic syntactic and semantic notions of the logic $L_{\infty\omega}$, we refer to Chapter A.2. It is important for us that we construe formulas as *sets*. Symbols in the basic language L may be urelements but we construe the formulas $\exists x \varphi$, $\forall \Theta$, etc. as the sets $\langle \exists, x, \varphi \rangle$, $\langle \forall, \Theta \rangle$, etc., with $\exists$, $\forall$ being some such fixed sets as 2 and 3. In such a set-up, proper subformulas of a formula φ are elements of $\text{TC}(\varphi)$ which fact makes it possible to give a

definition by TC-induction of the notion “ φ is a formula of the ∞, ω -logic based on L ”. In fact, by 2.18 we obtain that this notion is a Δ -predicate in KPU, more precisely, that there is a Δ -predicate symbol in KPU whose interpretation on V_U is that in quotes.

The last fact has an important consequence for *admissible fragments* of $L_{\infty\omega}$. Let A be an admissible set and let $L \in A$. We denote by L_A the collection of formulas of $L_{\infty\omega}$ that are in A , $L_A = L_{\infty\omega} \cap A$, and we call L_A an *admissible fragment* (of $L_{\infty\omega}$). By the absoluteness of Δ -predicates in KPU, 2.14, the Δ -definition of $L_{\infty\omega}$ when “relativized” to A , gives a definition of L_A , hence the notion of formula in L_A is Δ on A . Similarly, it turns out that the usual syntactic properties and operations on formulas of $L_{\infty\omega}$ are Δ in KPU, hence the corresponding notions for L_A are Δ on A .

Let A be admissible and a bit more generally than before, let the language L be a Δ_A -subset of A . Similarly as before, we can again see that the notion of formula in $L_A = L_{\infty\omega} \cap A$ and other syntactic notions of L_A are Δ on A . Notice that now for any $\varphi \in L_A$ there is an A -finite $L_0 \subseteq L$ such that $\varphi \in (L_0)_A$.

Returning to the “formal-in-KPU” context, we note next that actually the semantics of $L_{\infty\omega}$ is Δ in KPU as well. In other words, there is a Δ -predicate $\text{Sat}(L, \mathcal{M}, a, \varphi)$ of KPU expressing “ a is a finite sequence of elements of the L -structure $\mathcal{M}$ and $\mathcal{M} \models \varphi(a)$ ”, i.e., Sat when interpreted in V_U coincides with the predicate in quotes. Moreover, Sat satisfies, provably in KPU, the inductive clauses of the usual truth definition for $L_{\infty\omega}$. These facts are simply a special case of 2.18 again. Although these facts are very important, their importance is limited by the circumstance that in discussing an admissible fragment L_A we usually cannot restrict our attention to models in A itself. At any rate, it follows from the above that truth of L -formulas in an A -finite structure is a Δ -predicate on A , if A is admissible.

3. Examples of admissible sets. The truncation lemma

Some admissible sets

We made the remark earlier that the hereditarily finite sets, in any V_U , form an admissible set. Generalizing this remark, let κ be any infinite cardinal and define $H_U(\kappa) = \{a \in V_U \mid \text{TC}(a) \text{ has cardinality less than } \kappa\}$. $H(\kappa)$ is $H_\theta(\kappa)$.

3.1. THEOREM. *For all infinite cardinals κ , $H_U(\kappa)$ is admissible. If κ is regular, then $H_U(\kappa)$ is admissible relative to any predicates on it.*

PROOF The proof will follow from results below. $\square$

The reader will see that the case of regular κ is practically trivial. A regular κ has the added advantage that if $X \subset H_U(\kappa)$ and $\text{card}(X) < \kappa$, then $X \in H_U(\kappa)$.

For $\kappa = \aleph_1$, $H_U(\aleph_1)$ is denoted by HC_U , $H(\aleph_1)$ by HC , the set of hereditarily countable sets. The syntax of $L_{\omega_1\omega}$ is entirely within HC_U .

Let us write $\mathcal{M} <_1 \mathcal{N}$ to denote that $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$ with respect to Σ -formulas, i.e., $\mathcal{M} \models \varphi[a] \Leftrightarrow \mathcal{N} \models \varphi[a]$ for any Σ -formula $\varphi(x)$ and elements a in $|\mathcal{M}|$. When writing $A <_1 B$ for transitive sets, or classes, A, B we of course mean the corresponding structures with “real” $\in$ and “urelements”. The following is a classical result of LÉVY [1965].

3.2. LÉVY'S ABSOLUTENESS THEOREM. $H_U(\kappa) <_1 H_U(\lambda) <_1 V_U$ for uncountable cardinals $\kappa < \lambda$.

3.3. THEOREM. If A is a transitive set, B is an admissible set or class, and $A <_1 B$, then A is admissible as well.

Now we see that the first assertion in 3.1 is a consequence of 3.2 and 3.3.

3.4. THEOREM. Let κ be an infinite cardinal. For any $a \in H_U(\kappa^+)$, there is a transitive $A \in H_U(\kappa^+)$ such that $a \in A$ and $A < H_U(\kappa)$ (a fortiori, $A <_1 H_U(\kappa)$ and thus A is admissible).

PROOF. We expand the structure $\mathcal{M} = (H_U(\kappa^+), \in \upharpoonright H_U(\kappa^+), \cup \cap H_U(\kappa^+))$ with κ new operations $\langle f_\alpha : \alpha < \kappa \rangle$ such that for any $0 \neq a \in H_U(\kappa^+)$, $TC(a) = \{f_\alpha(a) : \alpha < \kappa\}$. This is clearly possible. Now, we apply the Downward Löwenheim–Skolem Theorem (cf. Chapter A.2) to get an elementary substructure of power κ of $(\mathcal{M}, f_\alpha)_{\alpha < \kappa}$ containing a . The underlying set of the new structure will satisfy the requirements. $\square$

The last result gives us many countable (and other) admissible sets — but there are many left that are not obtained in this way. As we will point out (cf. 6.3 below) the admissible sets given by the next theorem fall into the latter category.

3.5. PROPOSITION (Existence of the next admissible set). For any set $a \in V_U$, $HYP(a) =_{\text{df}} \bigcap \{A : a \in A, A \text{ is admissible}\}$ is itself admissible. $HYP(a) = L_\alpha(TC(a))$ for some ordinal α . $\text{Card } HYP(a) = \max(\aleph_0, \text{card } TC(a))$.

Remark. $\text{HYP}(a)$ is sometimes denoted by a^+ .

PROOF The proof (and in fact, the statement of the second assertion) requires considering the constructible hierarchy, cf. BARWISE [1975]. $\square$

Let now $\mathfrak{M}$ be a structure of finite similarity type, $\mathfrak{M} = (\|\mathfrak{M}\|, R_1, \dots, R_l)$. Regarding the elements of $\|\mathfrak{M}\|$ as urelements, let us place ourselves within $V_{\|\mathfrak{M}\|}$. Inside $V_{\|\mathfrak{M}\|}$, we form the next admissible set $\text{HYP}(\mathfrak{M}) = \text{HYP}(\langle \|\mathfrak{M}\|, R_1, \dots, R_l \rangle)$, and we call it $\text{HYP}_{\mathfrak{M}}$, the admissible hull of $\mathfrak{M}$. Note that technically, $\text{HYP}(\mathfrak{M})$ and $\text{HYP}_{\mathfrak{M}}$ may differ; e.g. the first may not contain urelements at all. Also, it is easy to see that for any isomorphism $f: \mathfrak{M} \cong \mathfrak{N}$, we get an extension $f^*: \text{HYP}_{\mathfrak{M}} \cong \text{HYP}_{\mathfrak{N}}$ which is an $\{\in, U\}$ isomorphism.

As a consequence of a definability theorem of BARWISE [1975], Theorem 5.14, Chapter 2, we have:

3.6. THEOREM. *On $A = \text{HYP}_{\mathfrak{M}}$, $\Sigma = \Sigma$ with parameters in $\|\mathfrak{M}\| \cup \{\|\mathfrak{M}\|, R_1, \dots, R_l\}$.*

An ordinal α is called *admissible* if L_α , the set of sets constructible before α , is admissible. In the *recursion theory on admissible ordinals*, various special kinds of admissible ordinals (such as *recursively inaccessible*, *projectible*, etc.) play important roles. An ordinal α is called *stable* if $L_\alpha <_1 L$. Obviously, every stable ordinal is admissible. The same argument as in 3.4 gives us many countable stable ordinals. In Section 6 we will point out (without proof) the significance of the first stable ordinal $> \omega$ for effective descriptive set theory. For more on admissible ordinals, we refer to BARWISE [1975].

The truncation lemma

Let $A = (\|A\|, E, U)$ be an arbitrary structure of the language $\{\varepsilon, U\}$ and assume A satisfies the (modified) axiom of extensionality:

$$\begin{aligned} & \forall x \forall y [(\neg Ux \wedge \neg Uy \wedge \forall z (zEx \leftrightarrow zEy)) \rightarrow x = y] \\ & \wedge \forall x \forall y [Ux \rightarrow \neg yEx]. \end{aligned}$$

We call A an *extensional* structure. For any transitive set or class $A \subset V_U$, $(A, \in \upharpoonright A, U \cap A)$ is, of course, an extensional structure. Let A be an extensional structure, and $a \in \|A\|$. a is said to be *well-founded* (w.f.) in A if there is no infinite “descending” sequence $a_0 = a, a_1, a_2, \dots$ such that

$a_{n+1}Ea_n$ for $n < \omega$. The whole structure is said to be w.f. if every $a \in |A|$ is. It is a good exercise to check that A is well-founded iff it satisfies the “principle of proof by E -induction”: for any subset $B \subset |A|$, $(|A|, E, U, B)$ satisfies $\forall x (\forall y (yEx \rightarrow By) \rightarrow Bx) \rightarrow \forall x Bx$. For a w.f. extensional A , there is a corresponding principle of definition by E -recursion.

Clearly, the “standard” $\in$ -structures, based on transitive sets, are well-founded.

3.7. MOSTOWSKI COLLAPSING LEMMA. *Every w.f. extensional structure is isomorphic to a standard $\in$ -structure. The isomorphism is unique once its effect on urelements is specified.*

PROOF. For $A = (|A|, E, U)$ w.f. extensional, define by E -recursion $f(p) = p$ for $p \in U$ and $f(u) = \{f(b) : bEa\}$ for $a \in |A| - U$. f is the required isomorphism. The uniqueness is proved by E -induction. $\square$

Incidentally, using 3.7 and the Löwenheim–Skolem theorem, we can prove Lévy’s theorem 3.2.

The essentially unique standard $\in$ -structure in 3.7 is called the *transitive collapse* of A .

Now, let A be an arbitrary extensional structure. Let $WF(A) \subset |A|$ (the *well-founded part* of A) be the set of all w.f. elements of A . Clearly, $U^A \subset WF(A)$ and $x \in WF(A)$ and $yE^A x$ imply that $y \in WF(A)$. With E^A restricted to $WF(A)$, $WF(A) = (WF(A), E^A \upharpoonright WF(A), U^A)$ is a w.f. structure and it is extensional.

Next we introduce the model-theoretic notion of end-extension. Let A, B be structures interpreting the binary predicate symbol E , among others. B is said to be an *end-extension* of A if B is an extension of A in the ordinary sense and moreover, if $a \in |A|$ and $bE^B a$, then $b \in |B|$.

Examples. (1) For transitive sets, $A \subset B$, the $\in$ -structure B is an end-extension of A .

(2) For an extensional structure A , A is an end-extension of $WF(A)$. The following generalizes 2.6. We leave the proof as an exercise.

3.8. PROPOSITION. *Let B be an end-extension of A , a elements of $|A|$.*

- (i) *For any Δ_0 -formula $\varphi(x)$, $A \models \varphi[a] \Leftrightarrow B \models \varphi[a]$.*
- (ii) *For any Σ -formula $\varphi(x)$, $A \models \varphi[a] \Rightarrow B \models \varphi[a]$.*
- (iii) *For any Σ -formula $\varphi(x)$ and Π -formula $\psi(x)$, if both in A and B*

$\forall x [\varphi(x) \leftrightarrow \psi(x)]$ is true (φ defines “ Δ -predicates” in A and B), then $A \models \varphi[a] \leftrightarrow B \models \varphi[a]$.

Now we turn to studying the well-founded part of a model $A = (|A|, E, U)$ of KPU. The set-theoretical rank-function $r(\cdot)$ is a Σ -operational symbol in KPU and “ $r(x)$ is an ordinal” and “ $y \in x \Rightarrow r(y) < r(x)$ ” are provable in KPU. It follows that $a \in |A|$ is w.f. in A iff $r^A(a)$ is.

The following is quite a characteristic property of KPU, not shared by many stronger set theories.

3.9. TRUNCATION LEMMA. *If $A = (|A|, E, U)$ is a model of KPU, then $WF(A) \models \text{KPU}$, hence $WF(A)$ is isomorphic to an admissible set.*

PROOF. Δ_0 -separation for $WF(A)$ follows immediately from that for A . We will apply the fact that $a \in WF(A)$ iff $b \in WF(A)$ for every $b \in a_E =_{\text{df}} \{b : bEa\}$ several times. E.g., it follows easily from this that $WF(A)$ satisfies Pair and Union. It remains to prove Δ_0 -collection. Let $\varphi(x, y, z)$ be a Δ_0 -formula, $a, c \in WF(A)$, and assume that

(i) $WF(A) \models \forall x \in a \exists y \varphi(x, y, c)$.

First of all, by 3.8 (ii) this implies that $A \models \forall x \in a \exists y \varphi(x, y, c)$ and hence

(ii) $A \models \forall x \in a \exists y \in b \varphi(x, y, c)$ for some $b \in |A|$. If each “ordinal” in A is well-founded, then $WF(A) = A$ and there is nothing to prove. So, assume β is a non-standard (i.e., non-w.f.) “ordinal” in A . All the standard, i.e., w.f., “ordinals” in A are smaller than β . By (i), the y ’s can be chosen w.f., so we have

(iii) $A \models \forall x \in a \exists y [r(y) < \beta \wedge \varphi(x, y, c)]$.

By the axiom schema of foundation in KPU, there is a “smallest” “ordinal” in A , β_0 , satisfying (iii). But for every non-standard β there is another non-standard $\beta' <^A \beta$ (why?), so (iii) will hold for β' as well — so, β_0 must be standard! Now consider $b \in |A|$ such that $xEb' \Leftrightarrow x \in b$ & $r(x) < \beta_0$; b' exists by Δ_0 -separation. We have $b' \in WF(A)$ (why?). (ii) and (iii) for β_0 imply that A , hence $WF(A)$ as well (why?), satisfy $\forall x \in a \exists y \in b' \varphi(x, y, c)$. $\square$

From now on, let us denote by $WF(A)$ the transitive collapse of what $WF(A)$ was before.

Next we formulate some consequences of the truncation lemma in connection with next admissible sets.

3.10. COROLLARY. *Let $A = \text{HYP}(a)$ be a pure admissible set. For any $b \in A$, there is a sentence $\varphi_{(a,b)}$ in the fragment L_A for some language L ,*

A-recursively depending on *a* and *b*, such that for any Σ -formula ψ , $H \models \psi[b] \Leftrightarrow \text{KPU} + \varphi_{(a,b)} \models \psi(b)$.

3.10 says that the truth of a Σ -formula in *A* can be “reduced” to the logical consequence relationship in L_A . We will compare 3.10 to other results later. Corollary 3.10 has a proof roughly similar to that of the next result whose proof we will sketch.

We call a relation $B \subset |\mathcal{M}|^n \Pi_1^1$ on $\mathcal{M}$ if there is a second order formula $\forall P_1 \cdots \forall P_k \psi(x, y, P)$, with a finitary first order formula ψ over the language $\{R, P\}$, such that for some parameters p in $|\mathcal{M}|$, we have $a \in B \Leftrightarrow \mathcal{M} \models \forall P_1 \cdots \forall P_k \psi[a, p]$.

3.11. COROLLARY. *For an infinite structure $\mathcal{M}$ of a finite similarity type, every relation on $|\mathcal{M}|$ that is Σ on $\text{HYP}_{\mathcal{M}}$ is Π_1^1 on $\mathcal{M}$.*

PROOF (outline). Notice that by the truncation lemma and the definition of $\text{HYP}_{\mathcal{M}}$, any model $\mathcal{N}$ of KPU that “contains” $\mathcal{M}$ in a suitable sense, will be an endextension of $\text{HYP}_{\mathcal{M}}$. Using also the upward persistence of Σ -formulas, the truth of a Σ -formula in *A* becomes equivalent to truth in *all* models of KPU that “contain” $\mathcal{M}$. This indicates how the second order universal quantifiers appear. The precise proof also uses 3.6. $\square$

4. Hintikka sets, model existence and Σ -compactness

The basic method of constructing models is constructing them out of certain kinds of sets of formulas. These sets give a more or less complete description of not only what atomic formulas, but also what other formulas are true of each finite tuple of elements of the model. Perhaps Hintikka sets (cf. 4.1) are the most refined kind of a set of formulas among those that give rise to a canonical model construction, in the sense that their definition contains a certain minimum of requirements.

In the rest of this chapter, by “formula” we will mean a formula of $L_{\omega_1\omega}$, for some *L*, unless it is clear otherwise from the context (e.g., a Σ -formula will always mean a finitary one as before).

We say that a formula is in negation normal form (n.n.f.) if it is built up from atomic and negated atomic formulas using only $\wedge$, $\vee$, $\forall$ and $\exists$. It is an easy exercise to show that every formula is logically equivalent to one in n.n.f.

4.1. DEFINITION. Let H be a set of sentences in n.n.f., with at least one individual constant occurring in H . H is called a *Hintikka set* if the following conditions are all satisfied:

- (i) For any atomic formula θ , it is impossible that both θ and $\neg \theta$ belong to H .
- (iia) For any closed (variable free) term t (of the language of H), $t \approx t \in H$.
- (iib) For any atomic formula $\varphi(x)$ with at most x free, any closed terms t_1, t_2 , if $\varphi(t_1) \in H$ and $t_1 \approx t_2 \in H$, then $\varphi(t_2) \in H$.
- (iii) If $\wedge \Sigma \in H$, then $\varphi \in H$ for every $\varphi \in \Sigma$.
- (iv) If $\forall x \varphi(x) \in H$, then $\varphi(t) \in H$ for every closed term t .
- (v) If $\vee \Sigma \in H$, then $\varphi \in H$ for some $\varphi \in \Sigma$.
- (vi) If $\exists x \varphi(x) \in H$, then $\varphi(t) \in H$ for some closed term t .

4.2. PROPOSITION. For any Hintikka set H , there is a model $\mathfrak{M}$ of H such that every element of $|\mathfrak{M}|$ is the denotation of some closed term.

PROOF. Let L be the set of nonlogical symbols in H . Introduce the equivalence relation $\sim$ on closed terms by $t_1 \sim t_2 \Leftrightarrow_{\text{df}} t_1 \approx t_2 \in H$. By (ii), $\sim$ is in fact a congruence relation with respect to symbols in L , i.e., we can define an L -structure $\mathfrak{M}$ on the set $|\mathfrak{M}|$ of equivalence classes of $\sim$ by putting

$$(t_1/\sim, \dots, t_n/\sim) \in P^{\mathfrak{M}} \Leftrightarrow_{\text{df}} Pt_1 \cdots t_n \in H,$$

$$f^{\mathfrak{M}}(t_1/\sim, \dots, t_n/\sim) =_{\text{df}} ft_1 \cdots t_n/\sim.$$

(Since there is at least one individual constant, $|\mathfrak{M}|$ is non-empty.) By induction on the n.n.f. sentence φ , we now show that $\varphi \in H$ implies $\mathfrak{M} \models \varphi$. For negated atomic formula φ , we use condition (i). The easy induction steps using the rest of the conditions are omitted. $\square$

The “crude” version of the notion of Hintikka set involved in the next result will be useful too. We call L_B a *fragment* of $L_{\omega_1\omega}$ if it is a set of $L_{\omega_1\omega}$ -formulas such that

- (i) with any $\varphi \in L_B$, any subformula of φ belongs to L_B (L_B is closed under subformulas),
- (ii) L_B is closed under substitution of terms of L , for free variables,
- (iii) L_B is closed under finitary logical operations $\neg, \wedge, \vee, \rightarrow, \forall$ and $\exists$,
- (iv) whenever $\vee \Sigma \in L_B$, then $\vee \{ \vee \Sigma \rightarrow \varphi : \varphi \in \Sigma \}$ belongs to L_B ,
- (v) each atomic formula of L belongs to L_B .

Notice that each countable admissible fragment is trivially a fragment in this sense.

4.3. PROPOSITION. *Let L_B be a fragment of $L_{\omega_1\omega}$, $C \subset L$ a set of individual constants and T a set of sentences in L_B . Assume:*

- (i) *Every finite subset of T is satisfiable.*
- (ii) *If the sentence $\vee \Sigma$ is a valid disjunction and it belongs to L_B , then there is $\varphi \in \Sigma$ such that $\varphi \in T$.*
- (iii) *If $\exists x \varphi(x) \in L_B$ and it is a valid sentence, then $\varphi(c) \in T$ for some $c \in C$.*

Then T is complete in L_B , i.e., for any sentence φ in L_B , either $\varphi \in T$ or $\neg \varphi \in T$, and T has a model $\mathfrak{M}$ such that every element of $|\mathfrak{M}|$ is the denotation of some $c \in C$. $\mathfrak{M}$ is unique up to isomorphism.

PROOF. The proof is similar to that of 4.2. $\square$

Let L_A be an admissible fragment of $L_{\omega_1\omega}$, with a countable admissible set A . We now will show an application of 4.3 in the proof of Barwise's Σ Compactness Theorem, one of the main results of the whole subject. In the proof, we will use Barwise's Completeness Theorem, to be proved in the next section. Implicitly, the proof of completeness will involve the more refined notion of Hintikka set.

4.4. Σ -COMPACTNESS THEOREM (Barwise). *Let A be a countable admissible set. Let T be a set of sentences in L_A , and let T be Σ on A . If every A -finite subset of T is satisfiable, then T is satisfiable.*

PROOF. We will extend T to a set satisfying (i)–(iii) in 4.3. Let C be a countably infinite set of constants, not occurring in T . Let $\exists x_n \psi_n(x_n), \vee \Sigma_n$ ($n = 0, 1, 2, \dots$) be enumerations of all logically valid sentences of the respective kinds of the fragment $L_A(C)$, the set of sentences that are obtained by substituting elements of C for free variables in formulas in L_A (note that each ψ in $L_A(C)$ contains only finitely many constants from C). By induction on $n < \omega$, we will define the sets T_n such that (i) $T_n - T$ is a finite set of sentences of $L_A(C)$, and (ii) each A -finite subset of T_n is satisfiable. Put $T_0 = T$. Then by the hypothesis, (i) and (ii) are satisfied. Suppose T_n is defined. Pick any $c \in C$ such that c does not occur in T_n (by (i), only finitely many elements of C occur in T_n) and put $T' = T_n \cup \{\psi_n(c)\}$. Notice that by (i), T' is a Σ -set on A . Since $\exists x \psi_n(x)$ is valid, by (ii) for T_n it is easy to see that each A -finite subset of T' is satisfiable.

Now, let $\forall \Sigma = \forall \Sigma_n$, and assume, for “reductio ad absurdum”, that for every $\varphi \in \Sigma$, $T' \cup \{\varphi\}$ fails to be A -finitely satisfiable. This means that we have

$$A \models \forall \varphi \in \Sigma \exists a (“a \subset T' \ \& \ \neg (\wedge a \wedge \varphi) \text{ is logically valid}”).$$

The Barwise Completeness Theorem in its “abstract” version (to be proved in the next section) says that the predicate “ φ is a logically valid sentence in A ” is a Σ -predicate on A . Using completeness and the Σ -formula defining T' with a parameter b , we can find a Σ_1 -formula $\exists x \delta(\varphi, x, a, b)$, with δ being Δ_0 , expressing the part in quotes. By $A \models \forall \varphi \in \Sigma \exists a \exists x \delta(\varphi, x, a, b)$ and Δ_0 -collection we obtain that there is $c \in A$ such that

$$A \models \forall \varphi \in \Sigma \exists a \in c \exists x \in c \delta(\varphi, a, x, b).$$

Consider

$$d =_{df} \{a \in c : \exists \varphi \in \Sigma \exists x \in c \delta(\varphi, a, x, b)\}.$$

By Δ_0 -separation, $d \in A$. Let $a_0 = \bigcup d$; we have that $a_0 \in A$. Since for every $a \in d$, $A \models \exists x \delta(\varphi, x, a, b)$ for some $\varphi, a \subset T$ and thus a_0 is an A -finite subset of T . By the definition of a_0 , for every $\varphi \in \Sigma$, there is $a \subset a_0$ such that $a \cup \{\varphi\}$ is unsatisfiable, hence, a fortiori for every $\varphi \in \Sigma$, $a_0 \cup \{\varphi\}$ is unsatisfiable. But this means precisely that $a_0 \cup \{\forall \Sigma\}$ is unsatisfiable, contradicting the fact that T' is A -finitely satisfiable.

We have shown that there is $\varphi \in \Sigma$ such that $T' \cup \{\varphi\}$ is A -finitely satisfiable. Define $T_{n+1} = T' \cup \{\varphi\}$. This completes the definition of the sequence T_n , $n < \omega$.

Put $T_\infty = \bigcup_{n < \omega} T_n$. By inspecting the construction, we see that T_∞ satisfies the conditions of 4.3; (i) because every finite subset of T_∞ is a finite, hence an A -finite, subset of some T_n . By 4.3, T_∞ and T have a model. $\square$

5. Conjunctive game formulas

Some second order notions

A Σ_1^1 -formula over $L_{\omega_1 \omega}$ (or, over L_A) is a second order formula of the form $\exists \bar{R} \varphi(\bar{R})$ where $\bar{R}$ is a finite or infinite set of predicate and/or operation symbols, φ is a formula of $(L \cup \bar{R})_{\omega_1 \omega}$ (or, of $(L \cup \bar{R})_A$ and in this case $\bar{R}$ is A -finite as well). If $\bar{R}$ is $\{R_1, \dots, R_n\}$, we also write $\exists R_1 \cdots \exists R_n \varphi$. If the free variables of $\exists \bar{R} \varphi$ are x , $\exists \bar{R} \varphi = \exists \bar{R} \varphi(\bar{R}, x)$,

then $\mathcal{M} \models \exists \bar{R} \varphi(\bar{R}, a)$ for $a \in |\mathcal{M}|$ if (naturally) there are relations R on $|\mathcal{M}|$ corresponding to $R \in \bar{R}$ such that $(\mathcal{M}, R)_{R \in \bar{R}} \models \varphi(\bar{R}, a)$. Π_1^1 formulas are similar but have $\forall$ in place of the $\exists$. A Π_1^1 - or Σ_1^1 -formula without further qualification is one such over finitary logic, $L_{\omega\omega}$.

For a class K of similar structures, we will say that K is $L_{\omega_1\omega}$ -elementary, or L_A -elementary, or Σ_1^1 -over- $L_{\omega_1\omega}$, etc., if there is φ such that $\mathcal{M} \in K$ iff $\mathcal{M} \models \varphi$ and $\varphi \in L_{\omega_1\omega}$, or $\varphi \in L_A$, or φ is Σ_1^1 -over- $L_{\omega_1\omega}$, etc., resp. We say that K is an $L_{\omega_1\omega}$ -elementary class of countable structures if for some $\varphi \in L_{\omega_1\omega}$, $\mathcal{M} \in K$ iff $\mathcal{M} \models \varphi$ and $\mathcal{M}$ is countable. Similarly, for the other notions.

We say that K is Δ_1^1 over $L_{\omega_1\omega}$, etc., if K is both Σ_1^1 and Π_1^1 over $L_{\omega_1\omega}$, etc. In short, $\Delta_1^1 = \Sigma_1^1 \cap \Pi_1^1$.

Next, fix a structure $\mathcal{M}$ of similarity type L , let $\Phi(x, y)$ be a formula (of an unspecified logic) let p be parameters in $|\mathcal{M}|$ (corresponding to y) and let $B \subset |\mathcal{M}|^n$ be the relation defined by Φ with the parameter p : for $a \in |\mathcal{M}|^n$, $a \in B \Leftrightarrow \mathcal{M} \models \Phi[a, p]$. If Φ is finitary first order, B is called *elementary on $\mathcal{M}$* . If Φ is Π_1^1 , or Π_1^1 over L_A , etc., we call B Π_1^1 , or Π_1^1 over L_A , etc. as well. If Φ is in $L_{\omega_1\omega}$ or in L_A , B is called $L_{\omega_1\omega}$ -*elementary*, or L_A -*elementary*, resp. Taking $\mathcal{M} = \omega =_{df} (\omega, 0, 1, +, \cdot)$, and a finitary first order formula Φ , we obtain what is ordinarily called an *arithmetical* subset of ω . With $\Phi \Pi_1^1$ or Σ_1^1 , we obtain the Π_1^1 - or Σ_1^1 -subsets of ω . For a general $\mathcal{M}$, again $\Delta_1^1 =_{df} \Sigma_1^1 \cap \Pi_1^1$, in all possible meanings of Σ_1^1 and Π_1^1 .

As a third group of notions, we introduce second order generalizations of the notions in the second group. Let $\mathcal{M}$ be a fixed structure of similarity type L again, let $\Psi(S, y)$ be a formula (of an unspecified kind) containing an n -ary predicate symbol S ("predicate variable") not interpreted in $\mathcal{M}$ (but all other non-logical symbols in Ψ are interpreted in $\mathcal{M}$), and let p be some fixed parameter in $|\mathcal{M}|$. Let X be the set of n -ary relations S on $|\mathcal{M}|$ such that $(\mathcal{M}, S) \models \Psi(S, p)$. If Ψ is finitary first order, X is called *elementary on $\mathcal{M}$* . Again, we obtain corresponding second order notions as well. If Ψ is Π_1^1 over $(L \cup \{S\})_{\omega_1\omega}$, X is called Π_1^1 over $L_{\omega_1\omega}$ (!) on $\mathcal{M}$, etc. Instead of Π_1^1 over $L_{\omega_1\omega}$, we also write Π_1^1 (*boldface* Π_1^1), etc.

Let E be the topological space of n -ary relations on $\omega, 2^{\omega^n}$ with the ordinary product topology. E is homeomorphic to the Cantor discontinuum. Then for $X \subset E$, X is Borel, analytic or complement analytic in the classical sense (cf. Chapter C.8) iff X is $L_{\omega_1\omega}$ -elementary, Σ_1^1 , or Π_1^1 , respectively, on ω .

Classes of structures are "more general" than classes of sets, in the following sense. Let X be a class of n -ary relations on $|\mathcal{M}|$, p finitely many elements in $|\mathcal{M}|$ and consider the class $\tilde{X}$ of all structures that are isomorphic to $(\mathcal{M}, p, S)$ for some $S \in X$. Results on X can sometimes be

derived from those on $\tilde{X}$, for the following reason. For simplicity, let $\mathfrak{M} = \omega$. The following $L_{\omega_1\omega}$ -sentence φ_0 characterizes ω up to isomorphism:

$$\wedge \text{Diagram } \omega \wedge \forall x \vee \{x \approx \ulcorner n \urcorner : n < \omega\};$$

here $\ulcorner n \urcorner = 1 + \dots + 1$ is the formal term denoting n . Now, if X is defined by $\Psi(S, \mathbf{p})$, then $\tilde{X}$ is defined by $\varphi_0 \wedge \Psi(S, \mathbf{p})$; so, if X is Π_1^1 , Σ_1^1 or Δ_1^1 , so is $\tilde{X}$, etc. We will exploit this possibility several times.

Conjunctive game sentences

A conjunctive game formula, or a Vaught formula as we will call it sometimes, is a particular kind of Σ_1^1 -over- $L_{\omega_1\omega}$ -formula, but in a peculiar form. A Vaught formula has the form

$$\Phi(\mathbf{z}) = \forall u_1 \bigwedge_{k_1 \in K_1} \exists v_1 \bigvee_{l_1 \in L_1} \dots \forall u_n \bigwedge_{k_n \in K_n} \forall v_n \bigvee_{l_n \in L_n} \dots$$

$$\bigwedge_{n < \omega} \varphi^{k_1 l_1 \dots k_n l_n}(\mathbf{z}, u_1, v_1, \dots, u_n, v_n)$$

where $K_1, L_1, \dots$ are countable sets and $\varphi^{k_1 l_1 \dots k_n l_n}$ is an $L_{\omega_1\omega}$ -formula with the indicated free variables, for every $k_1 \in K_1, l_1 \in L_1, \dots$. The meaning of “ Φ is satisfied by $\mathbf{c}$ in $\mathfrak{M}$ ”, in notation $\mathfrak{M} \models \Phi[\mathbf{c} \text{ for } \mathbf{z}]$ is best explained by an infinite game played by two players $\forall$ and $\exists$ on the structure $\mathfrak{M}$. A play consists of an ω -sequence of moves. At move n (≥ 1), $\forall$ picks an element $a_n \in |\mathfrak{M}|$ (interpreting u_n) and an index $k_n \in K_n$ and $\exists$ replies by picking $b_n \in |\mathfrak{M}|$ (interpreting v_n) and $l_n \in L_n$. After move n is completed for all $n = 1, 2, \dots$, $\exists$ wins iff $\mathfrak{M} \models \bigwedge_{n < \omega} \varphi^{k_1 l_1 \dots k_n l_n}[\mathbf{c}, a_1, b_1, \dots, a_n, b_n]$. A winning strategy for $\exists$ in this game is a sequence $\langle f_n : n < \omega \rangle$ of functions, $f_n : |\mathfrak{M}| \times K_1 \times \dots \times |\mathfrak{M}| \times K_n \rightarrow |\mathfrak{M}| \times L_n$, such that for any play $\langle a_1, a_2, \dots \rangle$ of $\forall$, if $\exists$ always replies according to his strategy, i.e., by choosing b_n, l_n determined by $\langle b_n, l_n \rangle = f_n(a_1, k_1, \dots, a_n, k_n)$, then $\exists$ wins in the above sense. Finally, $\mathfrak{M} \models \Phi[\mathbf{c}]$ means that $\exists$ has a winning strategy in the game on $(\mathfrak{M}, \mathbf{c})$, associated with Φ .

Let us first make a series of easy remarks on conjunctive game sentences. First of all, one might want to consider a less regular prefix as the one exhibited, or some of the quantifiers $\forall, \exists$ and $\wedge, \vee$ (which can be considered quantifiers on the fixed sets K_n, L_n) might be entirely missing. In all of these cases, by inserting dummy variables one can easily bring the formula to the exact form exhibited.

This remark is valid even if one takes a finite prefix to begin with, and e.g., one considers a prenex formula. Then one realizes that the truth-

definition via the game interpretation is nothing but the familiar Skolem form, with Skolem functions for the existentially quantified variables. This remark easily leads to recognizing the Σ_1^1 character of conjunctive game sentences in general, but we will return to this point below.

For the next remark, let us start with the Vaught formula Φ exhibited above, and for simplicity, let us make it a *sentence*, i.e., z the empty sequence. Then for any fixed indices $k_1, \dots, l_n$ from $K_1, \dots, L_n$, resp., we consider the *truncated* game formula $\Phi^{k_1 \dots l_n}(u_1, \dots, v_n)$ obtained by deleting the quantifiers from the beginning up to and including $\exists v_n$. Let p be the deleted part of the prefix. Now, $p\Phi^{k_1 \dots l_n}(u_1, \dots, v_n)$ can now be interpreted in two ways; one is the original Φ and the other is “ p applied to $\langle \Phi^{k_1 \dots l_n}; k_1 \in K_1, \dots, l_n \in L_n \rangle$.” The reader should convince himself that the two meanings are actually the same.

As a next remark, we state:

5.1. PROPOSITION. *For the Vaught sentence Φ as above (for simplicity, $z = \emptyset$), $\mathcal{M} \models \Phi$ iff there are predicates $P^{k_1 \dots l_n}(u_1, \dots, v_n)$ ($n < \omega$, $k_1 \in K_1, \dots, l_n \in L_n$) on $|\mathcal{M}|$ such that the structure $\mathcal{M}'$ obtained by expanding $\mathcal{M}$ by these predicates satisfies the sentence*

$$\begin{aligned} & P^\emptyset \wedge \bigwedge_{1 \leq n < \omega} \left[\bigwedge_{k_1 \in K_1} \cdots \bigwedge_{l_{n-1} \in L_{n-1}} \forall u_1 \cdots \forall v_{n-1} P^{k_1 \dots l_{n-1}}(u_1, \dots, v_{n-1}) \right. \\ & \quad \left. \rightarrow \forall u_n \bigwedge_{k_n \in K_n} \exists v_n \bigvee_{l_n \in L_n} P^{k_1 \dots l_n}(u_1, \dots, v_{n-1}, u_n, v_n) \right] \\ & \wedge \bigwedge_{1 \leq n < \omega} \bigwedge_{k_1 \in K_1} \cdots \bigwedge_{l_n \in L_n} \forall u_1 \cdots \forall v_n \left(P^{k_1 \dots l_n}(u_1, \dots, v_n) \right. \\ & \quad \left. \rightarrow \bigwedge_{i \leq n} \varphi^{k_1 \dots l_i}(u_1, \dots, v_i) \right). \end{aligned}$$

PROOF. For the only if part, notice that one can take $P^{k_1 \dots l_n}$ to be $\Phi^{k_1 \dots l_n}$ as defined above. Conversely, supposing the $P^{k_1 \dots l_n}$ exist with the required properties, one defines by induction on n the functions

$$f_n : K_1 \times |M| \times \cdots \times K_n \times |M| \rightarrow L_n \times |M|$$

such that $P^{k_1 \dots l_n}(a_1, b_1, \dots, a_n, b_n)$ holds for any $a_1, \dots, a_n \in |M|$, $k_1 \in K_1, \dots, k_n \in K_n$ and for $\langle l_i, b_i \rangle = f_i(a_1, k_1, \dots, a_i, k_i)$. For this, one uses the first and second conjuncts of the sentence exhibited above. Using the last conjunct, it immediately follows that the f_n form a winning strategy for $\exists$. $\square$

We say that the Vaught formula Φ is A -finite (or is in A) if the family $\langle \varphi^{k_1, \dots, l_n} : n < \omega, k_1 \in K_1, \dots, l_n \in L_n \rangle$ is A -finite.

5.2. COROLLARY. *Any Vaught formula is logically equivalent to a Σ_1^1 -formula over $L_{\omega_1\omega}$. If A is an admissible set, and the Vaught formula Φ is A -finite (in particular, $\omega \in A$), then Φ is logically equivalent to a Σ_1^1 -over- L_A -formula.*

The first main result tells us that, as far as countable models are concerned, conjunctive game formulas have the same expressive power as Σ_1^1 -over- $L_{\omega_1\omega}$ -formulas. What makes us consider the more complicated notion of conjunctive game formulas is the fact that their special syntactic form lends itself to useful manipulations, in particular, the construction of the *approximations*, cf. below.

We will use the notation $\models' \varphi$ to indicate that φ is true in all countable models. By the Downward Löwenheim-Skolem Theorem for $L_{\omega_1\omega}$ (cf. Chapter A.2) for an $L_{\omega_1\omega}$ -sentence φ , $\models' \varphi$ is equivalent to $\models \varphi$.

5.3. GAME-FORM THEOREM. *For every Σ_1^1 -sentence $\exists \bar{R} \varphi(\bar{R})$ over $L_{\omega_1\omega}$ there is a Vaught sentence Φ involving only symbols from L such that $\models' \Phi \leftrightarrow \exists \bar{R} \varphi(\bar{R})$. If A is an admissible set, $\omega \in A$ and $\exists \bar{R} \varphi(\bar{R})$ is Σ_1^1 over L_A , then Φ can be chosen to be A -finite. Actually, there is a Σ operation on A giving a suitable Φ for any Σ_1^1 -over- L_A -sentence as argument.*

PROOF (HARNIK [1974]). We may assume that $\varphi(\bar{R})$ is in n.n.f. Let Δ be a countable *fragment* (cf. above) of $L(\bar{R})_{\omega_1\omega}$ containing $\varphi(\bar{R})$ and $x \approx y$ (for the purpose of the " A -finite" case of the theorem, we have to take Δ to be A -finite; the *smallest* fragment containing φ and $x \approx y$ will be suitable (*exercise*; this uses the fact that $L(\bar{R})$ is (can be taken to be) A -finite and that $\omega \in A$)). Let C be an infinite set of new individual constants and $\Delta(C)$ the set of sentences that are substitution instances of formulas in Δ with elements of C substituted for the free variables. Let D be the set of all closed terms of the language $L \cup \bar{R} \cup C$. Now, we claim that for any countable L -structure $\mathcal{M}$, $\mathcal{M} \models \exists \bar{R} \varphi(\bar{R})$ iff the following is satisfied.

(i) There is a Hintikka set (cf. 4.1) $\Theta \subset \Delta(C)$ and an onto function $f : D \rightarrow |\mathcal{M}|$ such that $\varphi(\bar{R}) \in \Theta$ and for all atomic formulas $\pi(v_0, \dots, v_n)$ of L , and all $c_0, \dots, c_n \in D$, $\mathcal{M} \models \pi[f(c_0), \dots, f(c_n)]$ iff $\pi(c_0, \dots, c_n) \in \Theta$, and either $\pi(c_0, \dots, c_n)$ or $\neg \pi(c_0, \dots, c_n)$ belongs to Θ .

In fact, if $\mathcal{M} \models \exists \bar{R} \varphi(\bar{R})$, i.e., $(\mathcal{M}, \bar{R}) \models \varphi$ for certain relations $\bar{R}$ on $|M|$, then let f be any onto function $C \rightarrow |\mathcal{M}|$ and define Θ to be the set of all

$\varphi(c_0, \dots, c_n) \in \Delta(C)$ in n.n.f. such that $\mathcal{M} \models \varphi[f(c_0), \dots, f(c_n)]$. It is easy to see that these choices will satisfy (i). Conversely, assume (i). Let $\mathcal{M}'$ be the canonical model of Θ , constructed in the proof of 4.2. Then $\mathcal{M}' \models \varphi(\bar{R})$. By the definition of $\mathcal{M}'$ and by (i), we see that the function $c^{\mathcal{M}'} \mapsto f(c)$ is an isomorphism of $\mathcal{M}' \upharpoonright L$ and $\mathcal{M}$, establishing $\mathcal{M} \models \exists \bar{R} \varphi(\bar{R})$.

Next we express condition (i) on $\mathcal{M}$ in the form of a Vaught sentence Φ . Φ is defined as

$$\Phi = \forall u_1 \bigvee_{c_1 \in D} \bigwedge_{d_1 \in D} \exists v_1 \bigwedge_{\theta_1 \in \Delta(C)} \bigvee_{\theta_1 \in \Delta(C)} \\ \forall u_2 \dots \left(\bigwedge_{n < \omega} N^{c_1 d_1 \theta_1 \dots \theta_n}(u_1, v_1, \dots, u_n, v_n) \right)$$

(in the prefix, blocks like $\forall u_1 \dots \bigvee_{\theta_1 \in \Delta(C)}$ appear for each $n = 1, 2, \dots$) and the formulas $N^{c_1 \dots \theta_n}$ are defined as follows. There are two cases. Either every one of the conditions (ii)–(v) below on $\langle c_1, \dots, \theta_n \rangle$ is satisfied (*case 1*) or not (*case 2*). In case 2, we put $N^{c_1 \dots \theta_n}$ to be identically false, $\vee \emptyset$. In case 1, we put

$$N^{c_1 \dots \theta_n}(u_1, \dots, v_n) = \\ = \bigwedge \{ \alpha(u_1, \dots, v_n) : \alpha \text{ is an atomic or negated atomic formula} \\ \text{of } L \text{ and } \alpha(c_1, d_1, \dots, c_n, d_n) \in \{ \theta_1, \dots, \theta_n \} \}.$$

The conditions are as follows; we put $\Theta_n = \{ \varphi, \theta_1, \dots, \theta_{n-1} \}$.

- (ii) For no atomic π , both π and $\neg \pi$ belong to Θ_n .
- (iii) If $\delta_n \in \Theta_n$ and $\delta_n = \vee \Psi$ or $\delta_n = \exists v \psi(r)$, then $\theta_n = \psi$ for some $\psi \in \Psi$, or $\theta_n = \psi(t)$ for some closed term t , resp.
- (iv) If $\delta_n \notin \Theta_n$ but either (a) δ_n is $t \approx t$ or (b) δ_n is $\varphi(t_2)$ such that $t_1 \approx t_2 \in \Theta_n$ and $\varphi(t_1) \in \Theta_n$ or (c) $\delta_n \in \Sigma$ for some Σ such that $\bigwedge \Sigma \in \Theta_n$ or (d) $\delta_n = \varphi(t)$ such that $\forall x \varphi(x) \in \Theta_n$, then $\theta_n = \delta_n$.
- (v) If $\delta_n \notin \Theta_n$, δ_n is an atomic formula of L and none of (iv) (a), (b), (c), (d) is the case, then $\theta_n = \delta_n$ or $\theta_n = \neg \delta_n$.

(Intuitively, Θ_n is an “initial segment” of a Hintikka set, δ_n is the next formula to handle and θ_n is the next formula to be put into the Hintikka set.)

Let's show that $\mathcal{M}$ satisfies (i) iff $\mathcal{M} \models \Phi$, for a countable $\mathcal{M}$. It is easy to see that (i) implies $\mathcal{M} \models \Phi$. Indeed, let Θ be a Hintikka set satisfying (i). This is how we define a strategy of $\exists$. $c_n \in D$ and $b_n \in |\mathcal{M}|$ (interpreting v_n) are to be chosen by $\exists$ so that $f(c_n) = a_n = \text{choice of } \forall \text{ interpreting } u_n$, and $f(d_n) = b_n$ where $d_n \in C$ is the choice of $\forall$ in move n . Finally θ_n is to be

chosen by $\exists$ always in Θ and satisfying the requirements (iii)–(v); that this is possible follows from the fact that Θ is a Hintikka set and $\{\varphi(t), \theta_1, \dots, \theta_{n-1}\}$ (chosen so far) is a subset of Θ . Again from the Hintikka character of Θ , we will have that (ii) is satisfied. By the rest of (i), we have that $\mathcal{M} \models N^{c_1 \dots c_n}[a_1, \dots, b_n]$, for any choices of $\forall$ and strategic choices of $\exists$, proving that the exhibited strategy is winning.

Suppose next that $\mathcal{M} \models \Phi$ and let us fix a winning strategy of $\exists$ in the corresponding game played on $\mathcal{M}$. Let the strategy of $\exists$ be pitted against a play of $\forall$ in which

(vi) $\forall$ exhausts $|\mathcal{M}|$ by choosing a_n (interpreting u_n) so that $|\mathcal{M}| = \{a_n : 1 \leq n < \omega\}$,

(vii) every element of C occurs as some d_n (chosen by $\forall$ at move n) and

(viii) every sentence in $\Delta(C)$ occurs infinitely often as some δ_n .

Then the resulting play will be a sequence

$$a_1, c_1, d_1, b_1, \delta_1, \theta_1, \dots$$

$$\forall \quad \exists \quad \forall \quad \exists \quad \forall \quad \exists$$

(with the players indicated) and it will give us $\Theta = \{\theta_n : 1 \leq n < \omega\} \cup \{\varphi\}$ that is a Hintikka set containing φ . Indeed, since we have

(ix) $\mathcal{M} \models N^{c_1 \dots c_n}[a_1, \dots, b_n]$ for each n , $N^{c_1 \dots c_n}$ cannot be identically false. Hence case 2 above does not occur (for the sequences $\langle c_1, \dots, \theta_n \rangle$ given by the play), hence all the conditions (ii)–(v) hold. By (ii), 4.1(i) will hold. By (iv) and (viii), 4.1(ii), (iii) and (iv) will hold: e.g., if $\forall x \varphi(x) \in \Theta$ and t is a closed term, then for some n , $\forall x \varphi(x) \in \Theta_n$ and $\varphi(t) = \delta_n$ (by (viii)), hence by (iv), $\theta_n = \varphi(t) \in \Theta$. By (iii) and (viii), we similarly conclude that 4.1(v) and (vi) hold for Θ , hence Θ is a Hintikka set indeed.

Furthermore, the set

$$f = \{\langle c_n, a_n \rangle : 1 \leq n < \omega\} \cup \{\langle d_n, b_n \rangle : 1 \leq n < \omega\} \subset D \times |\mathcal{M}|$$

has domain and range D and $|\mathcal{M}|$, respectively, by (vii) and (vi). By (ix), the definition of the $N^{c_1 \dots c_n}$, (v) and (viii) we obtain that

$$\mathcal{M} \models \pi[e_1, \dots, e_n] \quad \text{iff} \quad \pi(f_1, \dots, f_n) \text{ is in } \Theta,$$

whenever $\langle e_i, f_i \rangle \in f$, $\pi(x_1, \dots, x_n)$ is an atomic formula of L . This implies that f is a function and also that the last part of (i) holds. This completes showing that $\mathcal{M} \models \Phi$ implies (i).

We completed showing that $\models' \exists \bar{R} \varphi(\bar{R}) \leftrightarrow \Phi$. From the above, one can extract a proof that $\exists \bar{R} \varphi(\bar{R})$ implies Φ even on an uncountable structure $\mathcal{M}$ (*exercise*), but the converse direction does need the countability of $\mathcal{M}$.

It is routine to verify that Φ will have the additional properties as well. $\square$

Approximations of conjunctive game formulas

The usefulness of Vaught formulas is mainly based on their approximations invented by Vaught (but also consult the historical remark at the end of this section). Let Φ be the general Vaught sentence exhibited above; again, we take z to be the empty sequence, for the sake of simplicity. We will use the abbreviation $\bar{k}$ for $\langle k_1, \dots, l_n \rangle$ (hence, for $n = 0$, $\bar{k}$ is the empty sequence). For arbitrary $0 \leq n < \omega$, arbitrary $\bar{k} \in K_1 \times \dots \times L_n$ and an arbitrary ordinal α , we define the $L_{\infty\omega}$ -formula $\Phi_\alpha^{\bar{k}} = \Phi_\alpha^{\bar{k}}(u_1, \dots, v_n)$ by a simultaneous induction on α as follows:

$$\Phi_0^{\bar{k}} = \bigwedge_{i \leq n} N^{k_i} l_i,$$

$$\Phi_{\alpha+1}^{\bar{k}} = \forall u_{n+1} \bigwedge_{k_{n+1} \in K_{n+1}} \exists v_{n+1} \bigvee_{l_{n+1} \in L_{n+1}} \Phi_\alpha^{\bar{k}, k_{n+1}, l_{n+1}},$$

$$\Phi_\lambda^{\bar{k}} = \bigwedge_{\alpha < \lambda} \Phi_\alpha^{\bar{k}} \quad \text{for a limit } \lambda.$$

Clearly, for countable α , $\Phi_\alpha^{\bar{k}}$ is a formula of $L_{\omega_1\omega}$. Moreover, $\Phi_\alpha^{\bar{k}}$ as a function of Φ , $\bar{k}$ and α is a Σ -operation on any admissible set (by Σ -recursion). In particular, if A is admissible, if Φ is A -finite, so are all approximations $\Phi_\alpha^{\bar{k}}$ for $\alpha < \text{Ord}(A)$. We write Φ_α for $\Phi_\alpha^\emptyset$.

If the prefix of the Vaught formula is different from the standard form, the approximations are appropriately modified. E.g., if Φ is

$$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \dots \bigwedge_{n < \omega} \varphi^n(x_1, \dots, y_n),$$

then the approximations are

$$\Phi_0^n = \bigwedge_{i \leq n} \varphi^i(x_1, \dots, y_i),$$

$$\Phi_{\alpha+1}^n = \forall x_{n+1} \exists y_{n+1} \Phi_\alpha^{n+1},$$

$$\Phi_\lambda^n = \bigwedge_{\alpha > \lambda} \Phi_\alpha^n \quad \lambda \text{ limit}$$

5.4. THEOREM (VAUGHT [1973]). *With the above notation,*

- (i) For $\alpha > \beta$, $\models \Phi_\alpha^{\bar{k}} \rightarrow \Phi_\beta^{\bar{k}}$.
- (ii) For every α , $\models \Phi \rightarrow \Phi_\alpha$.

(iii) For every structure $\mathcal{M}$ of power $\leq \kappa$, $\mathcal{M} \models \Phi_{\kappa^+} \rightarrow \Phi$.

(iv) In fact, if A is admissible, and both Φ and the L -structure $\mathcal{M}$ are A -finite, then $\mathcal{M} \models \Phi_{\text{Ord}(A)} \rightarrow \Phi$.

PROOF (i) is left as an exercise.

(ad (ii)) Recall the “truncated” game-formulas $\Phi^{\bar{k}}(u_1, \dots, v_n)$. (ii) is proved as a special case of $\models \forall u_1 \dots v_n [\Phi^{\bar{k}} \rightarrow \Phi_{\alpha}^{\bar{k}}]$ which in turn is proved by a straightforward induction on α .

(ad (iii)) (iii) follows from (iv) (why?) but (iii) is easier to show than (iv).

(ad (iv)) We first prove the following fact:

$$\mathcal{M} \models \forall u_1 \dots v_n \left[\bigwedge_{\alpha < \text{Ord}(A)} \Phi_{\alpha}^{\bar{k}} \rightarrow \forall u_{n+1} \right. \\ \left. \bigwedge_{k_{n+1} \in K_{n+1}} \exists v_{n+1} \bigvee_{l_{n+1} \in L_{n+1}} \bigwedge_{\alpha < \text{Ord}(A)} \Phi_{\alpha}^{\bar{k}, k_{n+1}, l_{n+1}} \right];$$

here $k_1 \in K_1, \dots, l_n \in L_n$ and $\bar{k} = \langle k_1, \dots, l_n \rangle$. Let $a_1, \dots, b_n \in |\mathcal{M}|$ be arbitrary (interpreting $u_1, \dots, v_n$) and assume (contraposition!) that the formula after $\rightarrow$ does not hold for $a_1, \dots, b_n$, i.e.,

$$(v) \quad A \models \exists u_{n+1} \in |\mathcal{M}| \exists k_{n+1} \in K_{n+1} \forall v_{n+1} \in |\mathcal{M}| \forall l_{n+1} \in L_{n+1} \\ \exists \alpha [\text{Ord}(\alpha) \wedge “\mathcal{M} \models \neg \Phi_{\alpha}^{\bar{k}, k_{n+1}, l_{n+1}}(a_1, \dots, b_n, u_{n+1}, v_{n+1})”].$$

By the remarks made above on $\Phi_{\alpha}^{\bar{k}}$ as a function of α and $\bar{k}$, and by the Δ -character of the truth definition of $L_{\infty\omega}$ in KPU, it follows that “ $\dots$ ” is a Δ -predicate of all the variables involved, including α . The only unrestricted quantifier in (v) is $\exists \alpha$. Hence, by Σ -collection there is a set $x \in A$ such that in (v) $\exists \alpha$ can be replaced by $\exists \alpha \in x$; x can clearly be taken to be an ordinal $\alpha_0 < \text{Ord}(A)$. By (i), then $\exists \alpha$ can be actually eliminated and the subscript α can be replaced by α_0 . By the definitions involved, the conclusion thus obtained is identical to saying that $\mathcal{M} \models \neg \Phi_{\alpha_0+1}^{\bar{k}}[a_1, \dots, b_n]$, and this establishes the claim.

Now, assume that $\mathcal{M} \models \Phi_{\text{Ord}(A)}$, i.e., $\mathcal{M} \models \bigwedge_{\alpha < \text{Ord}(A)} \Phi_{\alpha}^{\theta}$. We will use 5.1. Define the predicate $P^{\bar{k}}(u_1, \dots, v_n)$ to be $\bigwedge_{\alpha < \text{Ord}(A)} \Phi_{\alpha}^{\bar{k}}$. The first conjunct of the sentence in 5.1 holds by the assumption, the second by the claim and the last by the definition of $\Phi_0^{\bar{k}}$. $\square$

Notice that 5.4(ii) and (iii) say that $\models' \Phi \leftrightarrow \bigwedge_{\alpha < \aleph_1} \Phi_{\alpha}$. Taking into account the game-form Theorem 5.3, we obtain:

5.5. COROLLARY. Any Σ_1^1 -over- $L_{\omega_1\omega}$ -class of countable structures is the intersection of $\aleph_1$ elementary-over- $L_{\omega_1\omega}$ -classes.

By remarks made at the beginning of this section, as a special case we have:

5.6. COROLLARY. *Every analytic set in the Cantor space is the intersection of $\aleph_1$ Borel sets.*

5.7. REMARK. One reason why we are missing admissible sets with $\text{Ord}(A) = \omega$ (i.e., $\omega \notin A$) is that the assumption $\omega \in A$ is used throughout this section. This could be avoided, however, at the cost of a little extra work. The main modification that would be required is to use A -rec. Vaught formulas instead of A -finite ones. Φ (as above) is called A -recursive iff for each $n \in \omega$ the function $F_n = \langle \varphi^{k_1 \dots k_n} : k_1 \in K_1, \dots, k_n \in L_n \rangle$ is A -finite and $\langle F_n : n < \omega \rangle$ is A -recursive. Then in 5.3, for any admissible set A , Φ can be chosen to be A -rec. for A -finite $\exists \bar{R} \varphi(\bar{R})$, and in fact, the “index” of the A -rec. Φ (in a suitable sense) is an A -rec. function of $\exists \bar{R} \varphi(\bar{R})$.

Next one notes that for A -rec. Φ the family $\langle \Phi_\alpha^k : \alpha < \text{Ord}(A), n < \omega, \bar{k} \in K_1 \times \dots \times L_n \rangle$ is an A -rec. function (in particular, each approximation $\Phi_\alpha^{\bar{k}}$ is A -finite, for $\alpha \in A$).

Also, 5.4(iv) remains true, for A -recursive Φ with essentially the same proof.

5.8. HISTORICAL REMARK. The material in this section has a complicated history. The game-form theorem, formulated for finitary Σ_1^1 -sentences, is due to SVENONIUS [1965]. Vaught discovered the present form, but then he actually realized that the present form is a consequence of Svenonius’ theorem (cf. VAUGHT [1973]). Meanwhile, and earlier than Vaught, MOSCHOVAKIS [1970] rediscovered a version of Svenonius’ theorem, although strictly speaking his result is weaker. However, Moschovakis discovered (cf. the same reference) a version of the approximations of game sentences earlier than Vaught; he used his version to give a proof of $\Pi_1^1 = \text{inductive}$ on a countable structure. The main difference between Moschovakis’ and Vaught’s works is that Moschovakis worked with a fixed structure. Accordingly, he essentially shows the game form theorem and the theorem on approximations, 5.4(iii), only in a “local” form. On the other hand, the proof of Vaught’s version is very close to Moschovakis’ proof. The same thing is happening in both; Vaught saw more of what this thing was. We can also say that Vaught’s work is a “uniform” version of that of Moschovakis.

6. Applications of game formulas; completeness

6.1. THEOREM. *Let A be an admissible set, $A \subseteq \text{HC}_U$ (hence, every set in A is countable). Then the truth-definition of A -finite Π_1^1 -sentences in A -finite models is a Σ -predicate on A . I.e., there is a Σ -formula $\sigma(x, y, z)$ such that for an A -finite Π_1^1 -sentence $\forall \bar{R} \varphi(\bar{R})$ and an A -finite structure $\mathcal{M}$,*

$$\mathcal{M} \models \forall \bar{R} \varphi(\bar{R})[a] \quad \text{iff} \quad A \models \sigma[\forall \bar{R}(\bar{R}), \mathcal{M}, a].$$

Moreover, the same σ works for all A containing ω .

PROOF. Of course, the claim is equivalent to saying that “ Σ_1^1 -truth is Π on A ”. This is an immediate consequence of our work in the last section. For $\exists \bar{R} \varphi(\bar{R})$ in A , let Φ be a Vaught-equivalent of $\exists \bar{R} \varphi(\bar{R})$; Φ is a Σ -function of $\exists \bar{R} \varphi(\bar{R})$ (cf. 5.3). For $\mathcal{M}$ in A , we have $\mathcal{M} \models \exists \bar{R} \varphi(\bar{R})$ iff $\mathcal{M} \models \Phi$ (since $\mathcal{M}$ is countable) iff for all ordinals $\alpha \in A$, $\mathcal{M} \models \Phi_\alpha$, by 5.4(iv). This proof is valid for the case $\omega \in A$; for the general case, use 5.7; now we should take seriously our vague remark on “indices” in 5.7. $\square$

6.2. BARWISE'S ABSTRACT COMPLETENESS THEOREM. *For A as in 6.1, the predicate “ φ is logically valid”, for sentences φ in L_A , is Σ on A , uniformly for all A*

PROOF (VAUGHT [1973]). Our proof will work only if $\omega \in A$ (but see the remarks below). By the downward Löwenheim–Skolem theorem, any sentence in $L_{\omega_1 \omega}$ is valid iff it is true for all structures with domain ν , for any $\nu \leq \omega$. ν itself is a structure with the empty similarity type. Let $\varphi \in L_A$, let $\bar{R}$ denote the set of non-logical symbols in φ . Then φ is logically valid iff $\forall \nu \leq \omega \nu \models \forall \bar{R} \varphi(\bar{R})$. Now apply 6.1. $\square$

Remark. If there is at least one infinite set in A , this proof can be saved. We have to use models with possibly non-standard interpretations of equality — but that is no loss. The remaining admissible sets are exactly the HF_U , for various U , and the logic is exactly finitary logic. Even in this case, the proof can be “saved” by “adjoining” an infinite set to A ; details are omitted.

Remark. Let us emphasize that 6.2 is *not* the full Completeness Theorem of Barwise (stated in the Introduction!). On the other hand it is interesting that the abstract completeness theorem for L_A plays a crucial role in the

model theory of L_A , much more so than in the model theory of ordinary first order logic.

Let $\text{Valid}_A(\varphi)$ denote the predicate “ φ is a logically valid A -finite sentence of some fragment L_A ”. There are countable admissible sets A such that Valid_A is Δ on A ; e.g., if $A <_1 \text{HC}$ (*exercise*). But next admissible sets behave like HF in this sense: Valid_A is not Δ , and in fact, it is a “complete” A -r.e. set. Let $A = a^+$ be a pure next admissible set with $\omega \in A$. Let $\varphi(x_1, x_2)$ be a Σ formula, let $B \subset A$ be the set defined by $\varphi(x_1, c)$ on A , c being an element of A . We will now refer to 3.10. The infinitary sentence $(\bigwedge \text{KPU} \wedge \varphi_{\langle a, b, c \rangle}) \rightarrow \varphi(b, c)$ is an A -rec. function of b, c and the formula φ . Denote this function by $\xi(b, c, \varphi)$. 3.10 says that $b \in B \Leftrightarrow \psi(b, c, \varphi) \in \text{Valid}_A$, expressing the “completeness” of the Σ predicate Valid_A with respect to all Σ predicates on A . Now, by the Cantor diagonal argument, the predicate $Q(d) \Leftrightarrow “d = \langle c, \varphi \rangle$ for some $c \in A$ and Σ -formula φ and $\xi(\langle c, \varphi \rangle, c, \varphi) \notin \text{Valid}_A”$ is not Σ . But of course, Q is Π , hence, the Σ predicate $\neg Q(d)$ is not Π , hence it is not Δ . Thus, *there is a Σ predicate on A that is not Δ , hence by the “completeness” of Valid_A , we have proved*

6.3. THEOREM. *For a pure countable next admissible set $A = a^+$ with $\omega \in A$, Valid_A is not Δ on A .*

Next we state the converse of 3.12 for countable $\mathfrak{M}$.

6.4. THEOREM (BARWISE [1975]). *Let $\mathfrak{M} = (|\mathfrak{M}|, R_1, \dots, R_t)$ be a countably infinite structure of a finite similarity type and let S be a relation on $|\mathfrak{M}|$. Let $A = \text{HYP}_{\mathfrak{M}}$.*

- (i) *If S is Π_1^1 over L_A on $\mathfrak{M}$, then S is Σ on A .*
- (ii) *S is Π_1^1 on $\mathfrak{M}$ iff S is Σ on $\text{HYP}_{\mathfrak{M}}$.*
- (iii) *S is Δ_1^1 on $\mathfrak{M}$ iff $S \in \text{HYP}_{\mathfrak{M}}$.*

PROOF. (ad (i)) This follows immediately from 6.1 since $\mathfrak{M} \in A$.

(ad (ii)) This follows from (i) and 3.12.

(ad (iii)) This follows from (ii) and the Δ -separation principle. $\square$

If $\mathfrak{M} = (\omega, 0, 1, +, \cdot)$, then $\text{HYP}_{\mathfrak{M}}$ is, for all practical purposes, the same as $\text{HYP}(\omega)$; e.g. the pure sets in HYP_{ω} are exactly those in $\text{HYP}(\omega)$ (*exercise*). So we obtain the following result.

6.5. COROLLARY (KRIPKE [1964], PLATEK [1966]). *The Π_1^1 subsets of ω are exactly those subsets of ω that are $\text{HYP}(\omega)$ -r.e. The Δ_1^1 subsets of ω are exactly the $\text{HYP}(\omega)$ -finite subset of ω .*

To emphasize the historically very important 6.5, we give a concrete description of $\text{HYP}(\omega)$. Let us call an ordinal α recursive if there is a recursive ordering of a subset of ω having order-type α . Note that if α is a recursive ordinal and $\beta < \alpha$, then β is recursive too. Let ω_1^{CK} denote the first non-recursive ordinal.

6.6. THEOREM (KRIPKE [1964], PLATEK [1966]). $\omega^+ = L_{\omega_1^{\text{CK}}}$, i.e. the first admissible ordinal $> \omega$ is ω_1^{CK} .

PROOF. Let $\text{HYP}(\omega) = L_\alpha(\omega) = L_\alpha$. By the Σ -recursion theorem, it is easy to show that the order type of a well-ordering in an admissible set belongs to the admissible set itself. Since all recursive sets belong to $\text{HYP}(\omega)$ (exercise), it follows that $\omega_1^{\text{CK}} \leq \alpha$.

Now assume that $\omega_1^{\text{CK}} < \alpha$, i.e., $\beta = \omega_1^{\text{CK}} \in \text{HYP}(\omega)$. We use the notation W_e for the e th r.e. set and the following classical facts:

- (i) for every Π_1^1 set $A \subset \omega$, there is a recursive function f such that $n \in A \Leftrightarrow f(n)$ is the index of a recursive well-ordering $W_{f(n)}$ of a subset of (Suslin–Kleene normal form, cf. Chapter C.8), and
- (ii) there is a Π_1^1 set $C \subset \omega$ that is not Σ_1^1 (cf. Chapter C.8).

Let B be a Π_1^1 subset of ω that is not Σ_1^1 , and apply (i). Since for each $n \in B$, the order type of $W_{f(n)}$ is $< \beta$, there is an order preserving map g of the ordering $W_{f(n)}$ into $(\beta, \in | \beta)$. Of course, the existence of such a g implies that $n \in B$. The existence of g can be expressed by saying that an A -finite structure, A -recursively depending on n , will satisfy a certain Σ_1^1 -sentence over L_A (exercise). Putting those facts together with (the dual of) 6.1, we obtain that B is Π on A , hence by (the dual of) 6.5 that B is a Σ_1^1 subset of ω , which is a contradiction.

6.6'. COROLLARY. *The Δ_1^1 subsets of ω are exactly those that are constructible before ω_1^{CK} .*

Remark. Corollary 6.6' is a version of Kleene's theorem (KLEENE [1955]), one of the most important results of effective descriptive set-theory and (applied) second order logic. Kleene's theorem says that a subset of ω is hyperarithmetic iff it is Δ_1^1 . If we change Kleene's definition of hyp. to "to be an element of $L_{\omega_1^{\text{CK}}}$ ", 6.6' amounts to the modified Kleene theorem.

Actually, the two definitions of hyp. are similar; both involve a hierarchy indexed by recursive ordinals. As we see, 6.5 generalizes to arbitrary countable structures in 6.4. Kleene's theorem itself is a more refined and deeper statement that does not similarly generalize. Cf. a discussion of this point in MOSCHOVAKIS [1974].

We now state without proof a result that shows what role the first stable ordinal σ_0 plays in effective descriptive set theory.

- 6.7. THEOREM.** (i) σ_0 is the first non- Δ_2^1 -ordinal, i.e., the first ordinal α such that there is no Δ_2^1 well-ordering of a subset of ω with order type α .
 (ii) For $A = L_{\sigma_0}$, a subset B of ω is Σ_2^1 iff it is Σ on A .
 (iii) $B \subseteq \omega$ is Δ_2^1 iff $B \in A$.

We next state an important result whose proof uses the Barwise Completeness and Compactness Theorems, and also, the omitting types theorem (cf. Chapter A.2). A set a is called *internal* for a model $\mathfrak{N}$ satisfying the extensionality axiom if $a \in \text{WF}(\mathfrak{N})$. Let $A = \text{HYP}_{\mathfrak{M}}$, for a countable structure $\mathfrak{M}$. Let T be a theory in L_A , with $L = \{\in, U, \dots\}$, let T be Σ on A .

- 6.8. THEOREM.** *If a is internal for every model of T , then $a \in A$.*

Theorem 6.8 is a modern version of the Gandy–Kreisel–Tait Theorem: For any consistent Π_1^1 set of axioms for second order number theory, if $a \subseteq \omega$ is “in” every model of T , then a is hyperarithmetical.

For a proof and history of 6.8, cf. BARWISE [1975], Chapter 4, Theorem 1.3.

Finally, let us summarize the completeness and Σ -compactness Theorems for a countable admissible set A . The next theorem will be the basic tool in the next section on Σ -saturated structures. We leave its proof as an exercise.

- 6.9. THEOREM.** *Let T be a Σ_A theory in a countable admissible fragment L_A . Then for any $\varphi \in L_A$,*

- (i) $T \models \varphi$ iff for some A -finite T' , $T' \models \varphi$,
 (ii) $\{\varphi \in L_A : T \models \varphi\}$ is Σ on A (extended completeness)
 (iii) Let $p \subset I \times L_A$ be Σ_A family such that for each $i \in I$, $p_i = \{\psi : \langle i, \psi \rangle \in p\}$ is a set of L_A sentences. Then the family $\{\langle i, \varphi \rangle : i \in I, p_i \models \varphi\}$ is Σ on A (uniform extended completeness).

7. Σ -saturated structures

Throughout this section, A is a countable admissible set, L is a language that is a Δ subset of A . A Σ -family of L_A -types with parameters x is, by definition, a Σ set p such that $p \subset I \times L_A$ for some A -finite index-set I , and if $\langle i, \psi \rangle \in p$, then $\psi = \psi(v, x)$ is an L_A -formula with the free variables indicated. For $i \in I$, let p_i , or $p_i(v, x)$, be the “type” $\{\psi(v, x) : \langle i, \psi \rangle \in p\}$; p_i is a Σ set of formulas.

Let $\mathcal{M}$ be an L -structure and consider a Σ_A -family of L_A -types with parameters in $\mathcal{M}$, i.e., with some elements a in $|\mathcal{M}|$ (or, constants denoting them) substituted for x which were the parameters before. We talk about a family of types over $\mathcal{M}$. We say that p is realized in $\mathcal{M}$ if, using the above notation p_i , $\mathcal{M} \models \exists v \bigvee_{i \in I} \wedge p_i(v, a)$ i.e., at least one type p_i in the family is realized.

7.1. DEFINITION (RESSAYRE [1976], in present form: HARNIK [1974]). $\mathcal{M}$ is Σ_A -saturated iff for every Σ_A -family p of types over $\mathcal{M}$, if every A -finite subfamily $q \subseteq p$ is realized in $\mathcal{M}$, then p itself is realized in $\mathcal{M}$; in notation

$$\mathcal{M} \models \left[\bigwedge_{\substack{q \subseteq p \\ q \in A}} \exists v \bigvee_{i \in I} \wedge q_i(v, a) \right] \rightarrow \exists v \bigvee_{i \in I} \wedge p_i(v, a).$$

Remarks. In case I is a singleton, the infinite disjunction disappears and we obtain a condition formally close to the familiar $\aleph_0$ -saturation of model theory. In fact, for $A = \text{HF}$, we obtain what is called recursive saturation (actually, r.e.-saturation, but the two are equivalent) in Chapter A.2. Since a finite set I is not essentially more general than a singleton (*exercise*), Σ_{HF} -saturated = recursively saturated.

An equivalent definition of a Σ -saturated model is obtained by “breaking up” the original definition into two parts. The first part is the original condition with I a singleton (this condition is called Σ -saturation by SCHLIPF [1976], actually more appropriately than the full condition) and the second part is obtained by deleting x and $\exists x$ from the original (this second condition is called A -regularity by SCHLIPF [1976]).

The reader will see that in the proof of 7.2 below, it is A -regularity that is needed “to handle disjunctions”.

Every finite L -structure is Σ_A -saturated. For any set a , the structure (a) of the empty similarity type is Σ_A -saturated (*exercise*: note the scarcity of definable subsets of (a) in finitely many parameters). There are many Σ_A -saturated structures as Corollary 7.3 shows. The following is the fundamental theorem on Σ -saturated structures.

7.2. THEOREM (Strong relation universality of Σ -saturated structures, RESSAYRE [1976]). *Let T' be a Σ_A -theory in a language L'_A such that $L' \supseteq L$. If $\mathcal{M}$ is a countable Σ_A -saturated L -structure satisfying all L_A -consequences of T' , then $\mathcal{M}$ has a Σ_A -saturated expansion $\mathcal{M}'$ (i.e., $\mathcal{M}' \upharpoonright L = \mathcal{M}$) that is a model of T' .*

PROOF (HARNIK [1974]). Enlarge the language L' to $L'(|\mathcal{M}|)$ by introducing names for the elements of $|\mathcal{M}|$. The name of $a \in |\mathcal{M}|$ will also be denoted by a . Let $p^0, p^1, \dots, p^n, \dots$ be a list of all Σ_A -families $p(v, a)$ of L'_A types over $\mathcal{M}$ (note that A and $\mathcal{M}$ are countable). We will define by induction the sets $\Theta_0 \subset \Theta_1 \subset \dots$ such that, among others, we have (i) and (ii) below.

(i) Θ_n is a Σ_A set of $L'_A(|\mathcal{M}|)$ -sentences involving altogether only finitely many constants from $|\mathcal{M}|$ (notice that because of this condition, there is no difficulty with the meaning of Θ_n being Σ_A even though $|\mathcal{M}|$ is not a subset of A : one replaces the finitely many constants with finitely many free variables).

(ii) If $\Theta_n \models \psi(a)$, $\psi(x)$ is an L_A -formula, and $a \in |\mathcal{M}|$, then $\mathcal{M} \models \psi[a]$. Our aim is to construct the Θ_n so that $\bigcup_{n < \omega} \Theta_n$ will define (by 4.3) a model of T' that will be isomorphic to a Σ_A -saturated expansion of $\mathcal{M}$.

Put $\Theta_0 = T'$. (i) and (ii) are satisfied by the assumptions of the theorem.

Assume Θ_n has been defined. Let $p^n = p(v, a) \subset I \times L'_A$ be the n th family of types to be considered, a a list of all $|\mathcal{M}|$ constants involved in either Θ_n or p^n . In constructing Θ_{n+1} , we make sure that the saturation condition will hold for p^n .

For $i \in I$, define $r_i(v, a) = \{\psi(v, a) : \psi(v, x) \text{ is an } L_A\text{-formula (!) and } \Theta_n \cup p_i(v, a) \models \psi(v, a)\}$. By the extended completeness theorem (6.9(ii)), each r_i is a Σ_A set, and actually, by uniform extended completeness (6.9(iii)),

$$r = \{\langle i, \psi \rangle : \psi \in r_i, i \in I\}$$

is a Σ_A family of types. Consider the following cases:

Case 1. $\mathcal{M}$ realizes the family r . Let $b \in |\mathcal{M}|$ and $i \in I$ be such that $\mathcal{M} \models \bigwedge r_i(b, a)$. Take $\Theta_{n+1} = \Theta_n \cup p_i(b, a)$. Notice that, by the definition of r_i , conditions (i) and (ii) continue to hold for Θ_{n+1} .

Case 2. $\mathcal{M}$ does not realize r . Since $\mathcal{M}$ is Σ_A -saturated, there is an A -finite family $s \subset r$ such that s is not realized in $\mathcal{M}$. Since $s_i \subset r_i$ for each $i \in I$ and s_i is A -finite, we obtain by Σ -compactness that

$$(iii) \quad A \models \forall i \in I \exists t [t \subset p_i \wedge \Theta_n \models \forall v (\bigwedge t(v, a) \rightarrow \bigwedge s_i(v, a))].$$

By extended completeness, the predicate in brackets (of the variables t and i) is Σ on A . By Σ -collection, there is a set $w \in A$ such that for every $i \in I$, the t can be chosen in w , for every $i \in I$. But then for $q = (\bigcup w) \cap p$, we have

$$A \models \forall i \in I (q \subset p \wedge \Theta_n \models \forall v (\wedge q_i(v, a) \rightarrow \wedge s_i(v, a))).$$

In other words,

$$(iv) \quad \Theta_n \models \neg \exists v \bigvee_{i \in I} \wedge s_i(v, a) \rightarrow \neg \exists v \bigvee_{i \in I} \wedge q_i(v, a).$$

In case 2, let us put $\Theta_{n+1} = \Theta_n \cup \{\neg \exists v \bigvee_{i \in I} \wedge q_i(v, a)\}$. Since s is not realized in $\mathcal{M}$, the formula before $\rightarrow$ in (iv) is true in $\mathcal{M}$. Hence, by (iv), any L_A consequence of Θ_{n+1} is a consequence of Θ_n plus an L_A -sentence true in $\mathcal{M}$. But then the condition (ii) will be inherited from Θ_n to Θ_{n+1} . So (i) and (ii) hold again.

Having defined Θ_n for each $n < \omega$, put $\Theta_\omega = \bigcup_{n < \omega} \Theta_n$. We claim that Θ_ω satisfies (i)–(iii) in 4.3. The induction hypothesis (ii) implies that Θ_ω is finitely consistent. If $\bigvee \Phi$ is a valid disjunction in $L'_A(|\mathcal{M}|)$, then the Σ_A (in fact, A -finite) family $p \subset \Phi \times L'_A$ of types $p_\varphi = \{\varphi, v = v\}$ occurs as some p^n . When defining Θ_{n+1} , case 1 must occur since $\bigvee \Phi$ is valid. So $\Theta_{n+1} = \Theta_n \cup \{\varphi\}$ for some $\varphi \in \Phi$, establishing 4.3(ii) for Θ_ω . Checking 4.3(iii) is similar.

By 4.3, Θ_ω has a model $\mathcal{M}'$ each of whose elements is denoted by a constant in $|\mathcal{M}'|$ and such that $\mathcal{M}' \models \sigma$ iff $\sigma \in \Theta_\omega$, for $\sigma \in L'_A(|\mathcal{M}'|)$. Since for an L_A -formula $\psi(x)$, $\mathcal{M}' \models \psi(a)$ implies $\psi(a) \in \Theta_n$ for some $n < \omega$, hence by (ii), $\mathcal{M} = \psi[a]$, it follows that $a \mapsto a^{\mathcal{M}'}$ is an isomorphism of $\mathcal{M}$ onto $\mathcal{M}'|L$. Without loss of generality, we can assume that $\mathcal{M}'|L = \mathcal{M}$ and $a^{\mathcal{M}'} = a$. Since $\Theta_0 = T'$, $\mathcal{M}' \models T'$. Finally, let $p = p^n(v, a)$ be any Σ_A family of types over $\mathcal{M}'$. Notice that according to the construction of Θ_{n+1} , in case 1, p is realized in $\mathcal{M}'$ by the element b and in case 2, p is not even A -finitely realized in $\mathcal{M}'$. This means that $\mathcal{M}'$ is Σ_A -saturated. $\square$

7.3. COROLLARY (Existence of Σ -saturated models). *Any consistent Σ_A -theory T in L_A has a Σ_A -saturated model.*

PROOF. Take a finite or countable model $\mathcal{M}_0$ of T . Considering the structure $(|\mathcal{M}_0|)$ of the empty similarity type L_0 , every sentence of L_0 that is a consequence of T is true in $(|\mathcal{M}_0|)$. Since $(|\mathcal{M}_0|)$ is Σ_A -saturated, by 7.2 it has an expansion that is a Σ_A -saturated model of T . $\square$

An L -structure $\mathcal{M}$ is called Σ_A -relation universal if for every Σ_A theory

T' in L'_A , for some $L' \supseteq L$, if $\mathfrak{M}$ satisfies every L_A -consequence of T' , it has an expansion that is a model of T' . A weakening of 7.2 is:

7.4. COROLLARY (Σ_A -relation universality of Σ_A -saturated models). *Every Σ_A -saturated countable structure is Σ_A -relation universal.*

The Corollaries 7.3 and 7.4 by no means exhaust the full power of 7.2 as Ressayre's work amply demonstrates, although for many admissible sets A , Σ_A -relation universality does in fact characterize Σ_A -saturated models.

7.5. COROLLARY. *Any A -finite structure is Σ_A -saturated.*

PROOF. This is easy to prove directly, but it also follows from 7.3: one uses the sentence $\bigwedge \text{Diag}(\mathfrak{M}) \wedge \forall x \bigvee_{a \in |\mathfrak{M}|} x = a$ that characterizes $\mathfrak{M}$ up to isomorphism. $\square$

7.6. THEOREM (RESSAYRE [1976]). *Let $\mathfrak{M}$ be a countably infinite Σ_A -saturated structure of an A -finite language L . Let m be an infinite set, $m \in A$. Then there is an admissible set $B \supseteq A$ such that B contains an isomorphic copy of $\mathfrak{M}$ with underlying set m and such that $\text{Ord}(B) = \text{Ord}(A)$.*

PROOF (Outline; see HARNIK [1974]). Let T be a Σ_A -theory, in a language including $L, \in, U$, constants ' a ' for $a \in A$, and some other symbols, whose models, when reduced to $L \cup \{\in, U\}$, are exactly those $\mathfrak{N}$ whose $\in, U$ -reduct $\mathfrak{N}_1$ is a model of KPU such that $\mathfrak{N}_1$ is isomorphic to an end-extension of A and $\mathfrak{N}_1$ contains, as an "element", an isomorphic copy of the L -reduct of $\mathfrak{M}$ with underlying set m . Of course, any infinite L -structure can be expanded to a model of T . Since $\mathfrak{M}$ can be expanded to a model of T , by 7.2 it can be expanded to a Σ_A -saturated model $\mathfrak{N}$ of T (why?). We can assume that (the $\in, U$ -reduct of) $\mathfrak{N}$ is an end extension of A . The w.f. part of $\mathfrak{N}$ is an admissible set $B \supseteq A$ containing, as an element, an isomorphic copy of $\mathfrak{M}$ with underlying set m . It remains to show that $\text{Ord } B \leq \text{Ord } A$. Let a be any "ordinal" (if any) of $\mathfrak{N}$ such that each $\alpha < \text{Ord}(A)$ is "smaller" than a . Consider the Σ_a -type

$$\{ "v \text{ is an ordinal}" \} \cup \{ \alpha < v : \alpha < \text{Ord}(A) \} \cup \{ v < a \}.$$

It is clearly A -finitely satisfiable in $\mathfrak{N}$, hence by Σ -saturation, it is satisfiable in $\mathfrak{N}$. The conclusion is that among the "ordinals" a in $\mathfrak{N}$ that are "greater" than all $\alpha < \text{Ord}(A)$ there is no "smallest" one. Hence $\text{Ord}(A)$ cannot belong to B , hence $\text{Ord}(B) \leq \text{Ord}(A)$. $\square$

In the next theorem, we collect some results characterizing Σ_A -saturation for certain admissible sets A . We omit the proofs although they don't use anything going beyond the foregoing material.

7.7. THEOREM. *Let A be a resolvable countable admissible set, i.e., let A be the union of the range of an A -recursive function defined on the ordinals of A . Then the conclusion of 7.6 characterizes Σ_A -saturated structures of an A -finite similarity type. If $A = \text{HYP}(a)$ for a pure set a , $\mathfrak{M}$ is an L -structure, $L \in A$, then $\mathfrak{M}$ is Σ_A -saturated iff for $B = \text{HYP}(\{\mathfrak{M}, a\})$, considered in $V_{|\mathfrak{M}|}$, we have $\text{Ord}(B) = \text{Ord}(A)$. As a consequence, for such A , Σ_A -saturated structures are defined by a single Σ_1^1 -over- L_A sentence and they are also characterized by Σ_A -relation universality.*

In view of 7.7, we could have given alternative definitions of Σ_A -saturated structures, at least for certain A . In fact, the existence theorem 7.3, with one of these definitions of Σ -saturation, goes back to FRIEDMAN [1973]. But none of these definitions give us any hint why the following simple but fundamental property holds for Σ_A -saturated structures.

7.8. THEOREM. *The union of an L_A -elementary chain of Σ_A -saturated structures is Σ_A -saturated.*

PROOF. The proof is entirely trivial on the basis of the original definition. $\square$

Ressayre uses 7.8 along with 7.2 to give a new proof of Keisler's Theorem (KEISLER [1970]) saying that the set of logically valid sentences in $L_A(Q)$, the logic L_A augmented with the quantifier Qx "there are uncountably many $x \dots$ ", is Σ_A , for any countable admissible A . He also proves a general theorem that has the following theorem of GREGORY [1972] as a consequence: for any countable admissible A , if T is a Σ_A -theory in L_A , and T has a pair of models $\mathfrak{M}, \mathfrak{N}$ such that $\mathfrak{M} \not\leq_{L_A} \mathfrak{N}$, then T has an uncountable model.

Finally, let us give a proof of a theorem due to G. Sacks and proved subsequently in a simpler way by Friedman and Jensen, cf. also KEISLER [1971]. We call an ordinal α admissible if the set of constructible sets up to α , L_α , is admissible.

7.9. THEOREM (Sacks). *For every countable admissible ordinal α there is a subset a of ω such that $\alpha = \omega_1^a =_{\text{df}} \text{Ord}(\text{HYP}(a))$.*

PROOF (RESSAYRE [1976]). Let $A = L_\alpha$ be admissible. Let T be the Σ_A -theory in the language containing only the binary predicate symbol $<$ whose axioms are

(i) “ $<$ is a linear ordering”,

(ii) $_\beta$ “there is x such that $\{y: y < x\}$ has order type β ” for all $\beta < \alpha$ (it is a good exercise to show that there is an A -finite sentence expressing (ii) $_\beta$ and using only $<$ and $\approx$).

T is consistent, hence it has a Σ_A -saturated model $\mathcal{M}$. By 7.6, w.l.o.g. we can assume that $\mathcal{M} \in B$, $\mathcal{M}$ has universe ω , B is admissible, and $\text{Ord}(B) = \alpha$. $\mathcal{M}$ can be naturally identified with a subset $a \subset \omega$. It is obvious that for every $\beta < \alpha$, $\beta \in a^+$ but of course, $\alpha \notin a^+ \subset B$. Hence $\alpha = \text{Ord}(a^+)$. $\square$

Our two main applications of Σ -saturated structures will be given in the next two sections.

8. The covering theorem

Let A be a countable admissible set and let Φ be a conjunctive game sentence in A over a language $L \in A$. Recall the approximations Φ_β of Φ ; we will be interested in the Φ_β for $\beta < \text{Ord}(A)$. Each such Φ_β is a sentence of L_A and $\langle \Phi_\beta: \beta < \alpha \rangle$ is an A -recursive function. $\Phi \in A$ automatically implies that $\omega \in A$; for admissible sets with ordinal ω we should consider A -recursive conjunctive game sentences, cf. end of Section 5. The following theorem remains true, with essentially the same proof (based on earlier remarks) for the more general notion.

8.1. VAUGHT'S COVERING THEOREM (VAUGHT [1973]). *If φ is any sentence in L'_A for some $L' \supseteq L$, then $\Phi \models \varphi$ implies that $\Phi_\beta \models \varphi$ for some $\beta < \text{Ord}(A)$.*

PROOF (HARNIK [1974]). Using the heavy guns of the preceding sections, we can give a very short proof. Assuming that the conclusion is false, consider the consistent Σ_A -theory $\{\Phi_\beta: \beta < \text{Ord}(A)\} \cup \{\neg \varphi\}$. By 7.3, the theory has a countable Σ_A -saturated model $\mathcal{M}$. By 7.6, we can assume that $\mathcal{M} \in B$ for some admissible $B \supseteq A$ with $\text{Ord}(B) = \text{Ord}(A)$. Now, apply 5.4(iv) for the admissible set B and the B -finite structure $\mathcal{M}$. Since $\Phi_{\text{Ord}(B)} = \Phi_{\text{Ord}(A)} = \bigwedge_{\beta < \text{Ord}(A)} \Phi_\beta$, we have $\mathcal{M} \models \Phi_{\text{Ord}(B)}$, hence by 5.4(iv) $\mathcal{M} \models \Phi$. We have reached a contradiction since $\mathcal{M} \models \neg \varphi$ and $\Phi \models \varphi$. $\square$

This theorem is a fundamental theorem of logic. We will point out some

aspects of its importance below. We first state an immediate consequence of 8.1 and the game-form theorem 5.3.

8.2. STRONG CRAIG-LOPEZ-ESCOBAR INTERPOLATION THEOREM. (i) *Let $\varphi \rightarrow \psi$ be a valid implication of sentences in $L_{\omega_1\omega}$. Then there is a sentence θ in $L_{\omega_1\omega}$, a Craig interpolant of φ and ψ , such that $\varphi \rightarrow \theta$, $\theta \rightarrow \psi$ are both valid and all the non-logical symbols in θ occur both in φ and ψ . In fact, if $\varphi \in A$, $\psi \in B$, A, B are both admissible, $A \subset B$ and $\text{Ord}(A) = \text{Ord}(B)$, then θ can be found in A .*

(ii) *For any Σ_1^1 -sentence $\exists \bar{R} \varphi(\bar{R})$ over $L_{\omega_1\omega}$ there is an $\aleph_1$ -sequence $\langle \Phi_\alpha : \alpha < \aleph_1 \rangle$ of $L_{\omega_1\omega}$ -sentences such that whenever $\exists \bar{S} \psi(\bar{S})$ is any other Σ_1^1 sentence over $L_{\omega_1\omega}$ such that there is no (countable) model of $\exists \bar{R} \varphi \wedge \exists \bar{S} \psi$ ($\exists \bar{S} \psi$ is “disjoint” from $\exists \bar{R} \varphi$), then there is $\alpha < \aleph_1$ such that $\exists \bar{R} \varphi \models \Phi_\alpha$ and $\Phi_\alpha \models \neg \exists \bar{S} \psi$ (Φ_α “separates” $\exists \bar{R} \varphi$ and $\exists \bar{S} \psi$). In addition Φ_α is in the smallest admissible set containing $\exists \bar{R} \varphi$ and α , $\{\exists \bar{R} \varphi, \alpha\}^+$ for $\alpha < \aleph_1$. Also, for given $\exists \bar{S} \psi$, the α above can be found in $\{\exists \bar{R} \varphi, \exists \bar{S} \psi\}^+$.*

PROOF. (ad (ii)) Our proof will give the slightly weaker result with $\{\exists \bar{R} \varphi, \alpha, \omega\}^+$, $\{\exists \bar{R} \varphi, \exists \bar{S} \psi, \omega\}^+$ in the appropriate places. Using A -recursive Vaught sentences, we would get the full result. By the game-form theorem 5.3 there is a Vaught sentence Φ in $\{\exists \bar{R} \varphi, \omega\}^+$ such that Φ and $\exists \bar{R} \varphi$ are equivalent for countable models. Consider the approximations Φ_α for $\alpha < \aleph_1$. Given $\exists \bar{S} \psi(\bar{S})$ “disjoint” from $\exists \bar{R} \varphi$, we have $\Phi \models \neg \varphi(\bar{S})$, hence by the covering theorem there is $\Phi_\alpha \models \neg \varphi(\bar{S})$, i.e., $\Phi_\alpha \models \neg \exists \bar{S} \psi(\bar{S})$. Since $\Phi \models \Phi_\alpha$, also $\exists \bar{R} \varphi \models \Phi_\alpha$, hence $\exists \bar{R} \varphi \models \Phi_\alpha$ (why?). The covering theorem in fact gives α in any admissible set containing Φ , $\exists \bar{S} \psi(\bar{S})$ and thus, in any admissible set containing $\exists \bar{R} \varphi, \omega$ and $\exists \bar{S} \psi(\bar{S})$.

(ad (i)) Let L_0 be the set of the common non-logical symbols of φ and ψ , let $\bar{R}$ and $\bar{S}$ be the sets of non-logical symbols outside L_0 in φ and in ψ , respectively. Then $\models \varphi \rightarrow \psi$ is equivalent to saying that $\exists \bar{R} \varphi \models \neg \exists \bar{S} (\neg \psi)$. Applying (ii) we get the L_0 -sentence $\theta = \Phi_\alpha$ in $\{\exists \bar{R} \varphi, \alpha\}^+$ with $\alpha \in \{\exists \bar{R} \varphi, \exists \bar{S} (\neg \psi)\}^+$ such that $\models \varphi \rightarrow \theta \wedge \theta \rightarrow \psi$. With A and B as in the assumption, clearly $\theta \in A$.

Let us restate some direct consequences of 8.2 for emphasis.

8.3. COROLLARY (Suslin). *Disjoint analytic sets (of the Cantor-space) can be separated by a Borel set. In fact, given an analytic set A , there are $\aleph_1$ Borel sets B_α , $\alpha < \aleph_1$, such that $A = \bigcap_{\alpha < \aleph_1} B_\alpha$ and whenever A' is another analytic set disjoint from A , then some B_α separates A from A' .*

8.4. COROLLARY (Barwise Interpolation Theorem). *Two disjoint Σ_1^1 -over- L_A -classes of structures can be separated by an L_A -elementary class. Hence, Δ_1^1 -over- L_A - and L_A -elementary-classes coincide.*

Next, we formulate a second order generalization of 6.4(iii).

8.5. COROLLARY. *Let $\mathcal{M} = (|\mathcal{M}|, R_1, \dots, R_l)$ be a countably infinite structure and let X be a class of n -any relations on $|\mathcal{M}|$. Let $A = \text{HYP}_{\mathcal{M}}$ and $A_0 = L_{\text{Ord}(A)}$ (the smallest pure admissible set with the same ordinal as A). Then the following are equivalent:*

- (i) X is Δ_1^1 -over- L_A on $\mathcal{M}$.
- (ii) X is Δ_1^1 (-over- $L_{\omega\omega}$) on $\mathcal{M}$.
- (iii) X is L_A -elementary on $\mathcal{M}$.
- (iv) X is L_{A_0} -elementary on $\mathcal{M}$.

Remark. Notice that the implication (i) $\Rightarrow$ (iii) is a consequence of the Barwise interpolation theorem. On the other hand, by passing to $X = \{ \{n\} : n \in B \}$ from a subset B of ω , the equivalence (i) $\Leftrightarrow$ (iii) is a generalization of the second part of 6.5. This is how the Kleene Theorem (cf. the Remark after 6.6'), the Barwise interpolation theorem, and the Suslin separation theorem are related in the general result 8.2.

PROOF OF COROLLARY 8.5. First one establishes that Y is L_A -elementary on $M \Rightarrow Y$ is Π_1^1 on M . We omit the proof that is similar to that of 3.11. Then one sees that the implication (iii) $\rightarrow$ (ii) follows. “(ii) $\rightarrow$ (iii)” is contained in 8.4, but this is how we show the more refined “(ii) $\rightarrow$ (iv)”. Assume that X is Δ_1^1 on $\mathcal{M}$, $S \in X \Leftrightarrow (\mathcal{M}, S) \models \exists T_1 \varphi_1(S, T_1) \Leftrightarrow (\mathcal{M}, S) \models \forall T_2 \varphi_2(S, T_2)$, φ_1, φ_2 are finitary using some parameters $\mathbf{p}$ in $|\mathcal{M}|$. Now, let φ_0 be an A -finite sentence “describing” $\mathcal{M}$ in a language containing a constant for each $a \in |\mathcal{M}|$; φ_0 is

$$\wedge \text{Diag}(\mathcal{M}) \wedge \forall x \bigvee_{a \in |\mathcal{M}|} x = {}^r a {}^r$$

We have $\varphi_1(S, T_1) \models \varphi_0 \rightarrow \varphi_2(S, T_2)$ (why?). Hence, there is a Craig interpolant $\theta \in A_0$ (see 8.2(i)!) such that θ is over the language $\{R_1, \dots, R_l, S, \mathbf{p}\}$ and such that $\models \varphi_1 \rightarrow \theta$ and $\models \theta \wedge \varphi_0 \rightarrow \varphi_2$. Hence, $\theta(S, \mathbf{p})$ will define X on M (exercise). $\square$

The Lopez-Escobar generalization of Craig's interpolation theorem, 8.2(i) without the part “In fact, ...” was one of the first important results in

infinitary logic. Lopez-Escobar's proof was through a complete Gentzen-type infinitary formal system, quite similarly to Craig's original proof. Barwise established the same result for admissible fragments of $L_{\omega_1\omega}$. A natural proof of these results can be given using consistency properties, cf. KEISLER [1971]. The full strength of 8.2, however, does not seem to result from these proofs. RESSAYRE [1976] established the full 8.2 without using game-formulas (in fact, independently of VAUGHT [1973], but later) but Vaught's proof looks better to us.

The next corollary is a strong version of Beth's definability theorem (cf. e.g. Chapter A.2).

8.6. BETH'S THEOREM. *Let $\sigma(P)$ be a Σ_1^1 -sentence over $L(P)_A$ or more generally, let $\sigma(P)$ be $\exists \bar{R} \wedge \Psi(\bar{R}, P)$ for some Σ_A set Ψ of sentences in $L(\bar{R}, P)_A$. Suppose that on any L -structure $\mathfrak{M}$ there is at most one relation P such that $(\mathfrak{M}, P) \models \sigma$. Then there is an L_A -formula $\varphi(x)$ such that $\sigma \models \forall x (Px \leftrightarrow \varphi(x))$.*

PROOF Let $\sigma = \exists \bar{R} \psi(\bar{R}, P)$. Let $\bar{R}_1, \bar{R}_2$ be distinct copies of $\bar{R}$, P_1, P_2 of P , and a some individual constants. Then the hypothesis implies that the implication $[\psi(\bar{R}_1, P_1) \wedge P_1 a] \rightarrow [\psi(\bar{R}_2, P_2) \rightarrow P_2 a]$ is logically valid. The two sides of the implication have only L and a in common. By the interpolation theorem, there is an $L_A(a)$ formula $\varphi(a)$ that is a Craig interpolant. Then $\varphi(x)$ is the required L_A -definition of P . *Exercise:* Complete the proof for the more general kind of σ . $\square$

In the proof of the next theorem, we will utilize the exact form of Vaught's approximations.

8.7. THEOREM. *Let φ be a sentence of L_A, L containing a binary predicate symbol $<$. Suppose that for each $\beta < \text{Ord}(A)$, there is a model $\mathfrak{M}$ of φ such that $<^{\mathfrak{M}}$ is a linear ordering containing a subordering having order type β . Then φ has a model $\mathfrak{M}$ such that $<^{\mathfrak{M}}$ contains a copy of the ordering of the rational numbers.*

8.8. COROLLARY. *If each model of φ is well-ordered, then there is an ordinal $\beta \in A$ such that each model of φ has order type $\leq \beta$.*

8.9. COROLLARY. *The class of countable well-orderings is not a Σ_1^1 -over- $L_{\omega_1\omega}$ -class of countable structures.*

PROOF OF THEOREM 8.7. We will assume that in each model we talk about, $<$ automatically denotes a linear ordering (why can we do this?). We start by writing down a purely existential "Vaught sentence" whose models are precisely the extensions of $\mathbf{Q}$, the ordering of the rational numbers. Let $\{r_n: 1 \leq n < \omega\}$ be a repetition-free enumeration of $|\mathbf{Q}|$. Let $\delta(x_1, \dots, x_n)$ denote the conjunction

$$\bigwedge \{x_i < x_j: r_i < r_j, 1 \leq i, j \leq n\}.$$

Then the sentence Φ is

$$\exists x_1 \exists x_2 \cdots \exists x_n \cdots \bigwedge_{n < \omega} \delta_n(x_1, \dots, x_n);$$

Φ clearly serves our purposes. By contraposition, assume that φ does not have a model containing a copy of $\mathbf{Q}$. Then we have $\Phi \models \neg \varphi$. Note that $\Phi \in A$ whenever $\omega \in A$, and Φ is A -recursive always. By the covering theorem, there is $\alpha_0 < \text{Ord}(A)$ such that $\Phi_{\alpha_0} \models \neg \varphi$. By analyzing the meaning of Φ_{α_0} , we will obtain the desired conclusion, as follows.

Let us say that a linear ordering has length $\geq \alpha$ if it has a subordering of type α . Let $r_{i_1} < \cdots < r_{i_n}$ be the proper ordering of the first n rationals. We claim that for any ordinal α , and any ordering $\mathcal{M} = (|\mathcal{M}|, <^{\mathcal{M}})$, if $a_{i_1} <^{\mathcal{M}} \cdots <^{\mathcal{M}} a_{i_n}$ and each of the open intervals $(, a_{i_1}), (a_{i_1}, a_{i_2}), \dots, (a_{i_{n-1}}, a_{i_n}), (a_{i_n},)$ are of length $\geq 3^\alpha$, then $\mathcal{M} \models \Phi_\alpha^n[a_1, \dots, a_n]$. For $n = 0$, the hypothesis is understood to mean that $\mathcal{M}$ has length $\geq 3^\alpha$ and the conclusion is $\mathcal{M} \models \Phi_\alpha$. The proof is an induction on α . For $\alpha = 0$, the claim is easily seen. For $\alpha = \beta + 1$, $\Phi_\alpha(x_1, \dots, x_n) = \exists x_{n+1} \Phi_\beta(x_1, \dots, x_{n+1})$. We now look at which one of the intervals $(, r_{i_1}), (r_{i_1}, r_{i_2}), \dots, (r_{i_{n-1}}, r_{i_n}), (r_{i_n},)$ r_{n+1} falls into. Suppose e.g. $r_{i_k} < r_{n+1} < r_{i_{k+1}}$. Since $3^{\beta+1} \geq 3^\beta + 1 + 3^\beta$, there is $a = a_{n+1}$ such that $a_{i_k} <^{\mathcal{M}} a <^{\mathcal{M}} a_{i_{k+1}}$ and both (a_{i_k}, a) and $(a, a_{i_{k+1}})$ are of length $\geq 3^\beta$. Hence, by the induction hypothesis, $\mathcal{M} \models \Phi_\beta[a_1, \dots, a_n, a_{n+1}]$, hence $\mathcal{M} \models \Phi_{\beta+1}[a_1, \dots, a_n]$. For α a limit ordinal, the induction step is trivial.

The claim and $\Phi_{\alpha_0} \models \neg \varphi$ imply that whenever $\mathcal{M} \models \varphi$, then $\mathcal{M}$ does not have length $\geq 3^{\alpha_0}$. Since, as it is easy to see, $\alpha_0 \in A$ implies that $3^{\alpha_0} \in A$, this proves the theorem. $\square$

Cf. KEISLER [1971] for an alternative proof, using consistency properties. In BARWISE [1975] there is a proof that is a direct application of the Σ -compactness theorem.

We presented the above proof to illustrate a typical use of Vaught's covering theorem. In MAKKAÏ [1973] and HARNIK and MAKKAÏ [1975] there

are other applications of the covering theorem where the form and/or the meaning of the approximations play a role. Thus, the importance of the covering theorem is not contained in its main application, 8.2, but rather, it is important to use the exact form of the approximations in many cases. This is a fine example for in what sense a logical generalization (the covering theorem) supersedes the original descriptive set-theoretical result (Suslin's theorem).

In VAUGHT [1973], there are further results whose proofs are based on game-sentences and their approximations. We state two of them.

8.10. REDUCTION THEOREM FOR $L_{\omega_1\omega}$ (VAUGHT [1973]). *For any two Π_1^1 -over- $L_{\omega_1\omega}$ -classes K_1, K_2 of countably infinite structures, there are Π_1^1 -over- $L_{\omega_1\omega}$ -classes K_1^*, K_2^* such that $K_1^* \subseteq K_1$, $K_2^* \subseteq K_2$, $K_1^* \cap K_2^* = \emptyset$ and $K_1^* \cup K_2^* = K_1 \cup K_2$.*

8.11. THEOREM (VAUGHT [1973]). *Any Σ_1^1 -over- $L_{\omega_1\omega}$ - (and actually, Σ_2^1 -over- $L_{\omega_1\omega}$) class of countable structures is the union of $\aleph_1$ $L_{\omega_1\omega}$ -elementary classes.*

It turns out that Scott's isomorphism theorem (cf. SCOTT [1965]) is a direct consequence of 8.11. On the other hand, both results 8.10, 8.11 specialize to classical results of descriptive set-theory, e.g. the first to the reduction property of complement-analytic sets.

RESSAYRE [1976] contains further interesting applications of model theory to descriptive set-theory. Ressayre gives a proof of a characterization of Π_1^1 sets of subsets of ω using admissible sets, the Spector–Gandy theorem. Let $\mathcal{M} = (|\mathcal{M}|, R_1, \dots, R_l)$ be a countable structure of a finite similarly type.

8.12. SPECTOR–GANDY THEOREM. *A set X of subsets of $|\mathcal{M}|$ is Π_1^1 iff there is a Σ -formula $\sigma(x, y)$ and some parameters p in $|\mathcal{M}| \cup \{\mathcal{M}, R_1, \dots, R_l\}$ such that*

$$X = \{B \subseteq \omega : \text{HYP}_{(\mathcal{M}, B)} \models \sigma[B, p]\}.$$

Notice that 8.12 is a second-order generalization of 6.4(ii). Its proof is very similar to that of 6.4. Ressayre uses 8.12 (for $\mathcal{M} = (\omega, 0, 1, +, \cdot)$) to give a “model-theoretic” proof of the Novikov–Kondo uniformization theorem (cf. Chapter C.8).

9. The perfect subset theorem

A classical theorem of descriptive set-theory says that any uncountable analytic set, say of the Cantor discontinuum, contains a perfect subset, and hence has power $2^{\aleph_0}$ (cf. Chapter C.8).

On the other hand, a theorem in HARRISON [1966] (cf. also MANSFIELD [1970]) says that, if X is a countable light-face (for simplicity) Σ_1^1 set of subsets of ω , then each element of X is hyperarithmetic. We will prove a model-theoretic theorem that has both theorems as consequences. It also simultaneously generalizes the definability theorem of REYES [1970] (cf. also CHANG [1964], MAKKAJ [1964] and CHANG and KEISLER [1973]) and a theorem of KUEKER [1968].

Let A be a countable admissible set. Let $\theta = \{\theta_i(v, u_i) : i \in I\}$ be an A -finite family of L_A -formulas and suppose that an $L(P)$ -structure $(\mathcal{M}, P)$ satisfies the disjunction

$$\bigvee_{i \in I} \exists u_i \forall v (P(v) \leftrightarrow \theta_i(v, u_i)),$$

denoted shortly by δ_θ . Then P is defined by one of the formulas $\theta_i(v, b_i)$ with some parameters b_i in $|\mathcal{M}|$. Now, if for a sentence σ over $L(P)$ (in any "logic"), we know that $\sigma \models \delta_\theta$, then for any L -structure $\mathcal{M}$ and any P on $|\mathcal{M}|$ such that $(\mathcal{M}, P) \models \sigma$, the above conclusion holds. In particular, for a fixed countable L -structure $\mathcal{M}$, $\{P : (\mathcal{M}, P) \models \sigma\}$ will be a countable set. This shows the implication (iii) $\Rightarrow$ (i) in the following theorem.

9.1. THEOREM. *For a Σ_1^1 -sentence σ of form $\exists \bar{R} \wedge \Psi(\bar{R}, P)$, with a Σ_A set $\Psi(R, \bar{P})$ of sentences of $L(R, \bar{P})_A$ (in particular, σ can be a Σ_1^1 sentence over $L(P)_A$), the following are equivalent.*

- (i) *For every countable L -structure $\mathcal{M}$, $\{P : (\mathcal{M}, P) \models \sigma\}$ is countable.*
- (ii) *For every countable L -structure $\mathcal{M}$, $\{P : (\mathcal{M}, P) \models \sigma\}$ does not contain a perfect subset (in the Cantor space $2^{|\mathcal{M}|^n}$, if P is n -ary).*
- (iii) *For some A -finite θ as above, $\sigma \models \delta_\theta$.*

9.2. COROLLARY (HARRISON [1966]). *For a Σ_1^1 set X of subsets of ω , if X does not contain a perfect subset, every element of X is hyperarithmetic, in fact, X is a subset of an ω^+ -finite set.*

PROOF (based on 9.1). Let $\sigma(P)$ be the Σ_1^1 -sentence defining X on $\mathcal{M} = (\omega, 0, 1, +, \cdot)$. Apply (ii) $\Rightarrow$ (iii) for $A = \omega^+ = L_{\omega_1^{CK}}$. We obtain that for some A -finite $\theta = \{\theta_i : i \in I\}$,

$$X \subseteq Y =_{\text{df}} \{\{a \in \omega : \mathfrak{M} = \theta_i [a, b_i]\} : i \in I, b_i \in {}^\omega \omega\}.$$

$Y \subset A$, in fact Y is an A -finite set (why?). By 6.5, the assertion follows. $\square$

For a first-order sentence σ of $L(P)_A$, 9.1 was proved in MAKKAÏ [1973b]. Subsequently Barwise noticed the present more general (and more useful) form, cf. BARWISE [1975]. The proof in MAKKAÏ [1973b] as well as the one in BARWISE [1975] uses consistency properties ("consistency machines", in Barwise's words). The proof via 9.3 given below, using Σ -saturated structures, is due to HARNIK [1974]. The next theorem is a direct generalization of Harrison's theorem.

9.3. THEOREM (HARNIK [1974]). *Let σ be a Σ_1^1 -sentence $\exists \bar{R} \wedge \bar{\Psi}(\bar{R}, P)$, with $\bar{\Psi}(\bar{R}, P)$ a Σ_A set of sentences in $L(R, P)_A$ (in particular, σ can be a Σ_1^1 -sentence over $L(P)_A$). Let $\mathfrak{M}$ be a countable Σ_A -saturated L -structure and assume that there is $P_0 \subset |\mathfrak{M}|$ such that $(\mathfrak{M}, P_0) \models \sigma$ and P_0 is not L_A -elementary on $\mathfrak{M}$. Then $\{P : (\mathfrak{M}, P) \models \sigma\}$ contains a perfect subset.*

PROOF. Let $\sigma = \exists \bar{R} \wedge \bar{\Psi}(\bar{R}, P)$. Let $\Theta(P)$ be the set

$$\{\neg(\exists u \forall v (P(v) \leftrightarrow \theta(v, u))) : \theta \in L_A\}.$$

Clearly, $\Theta(P)$ is an A -recursive set. The hypothesis implies that $(\mathfrak{M}, P_0)$ is a model of $\{\sigma\} \cup \Theta(P)$. By induction, we are going to define finite sets $M_0 \subset M_1 \subset \dots \subset M_n \subset \dots$, $M_n \subset |\mathfrak{M}|$, and Σ_A sets $T_s(\bar{R}, P)$ of sentences of $L(\bar{R}, P)_A(|\mathfrak{M}|)$ (using finitely many constants denoting elements in $|\mathfrak{M}|$) for $s \in {}^\omega 2$ such that (i)–(iv) below hold:

(i) If $\text{lh}(s) = n$, then $T_s(\bar{R}, P) \subset L(\bar{R}, P)_A(M_n)$; if $s \subset s'$, then $\bar{\Psi} \subset T_s(\bar{R}, P) \subset T_{s'}(\bar{R}, P)$.

(ii) If s and s' are incomparable, then $T_s(\bar{R}, P) \cup T_{s'}(\bar{R}, P) \models P(a) \nleftrightarrow P'(a)$ for some constant $a \in M_n$, $n = \min(\text{lh}(s), \text{lh}(s'))$.

The definitions will be devised to ensure that for all $\eta \in {}^\omega 2$, $(\mathfrak{M}, a)_{a \in |\mathfrak{M}|}$ is a model of $\exists \bar{R} \exists P \wedge (\bigcup_{n < \omega} T_{\eta|n}(\bar{R}, P))$. This will produce a perfect set of P 's such that $(\mathfrak{M}, P) \models \sigma$. The essential induction hypothesis for the construction is

(iii)_n $(\mathfrak{M}, a)_{a \in M_n} \models \exists P \exists \bar{R} \wedge (T_s(\bar{R}, P) \cup \Theta(P))$ for all $s \in {}^\omega 2$. (This will ensure, among other things, that $\bigcup_{n < \omega} T_{\eta|n}(\bar{R}, P)$ is finitely consistent with $\text{Diag}(\mathfrak{M})$.) To formulate one more condition, let $\exists u \delta_0(u), \exists u \delta_1(u), \dots$ enumerate all valid sentences in $L(R, P)_A(|\mathfrak{M}|)$ of the form $\exists u \delta(u)$, and let $\vee \Psi_0, \vee \Psi_1, \dots$ enumerate all valid disjunctions in the same logic. The last useful property of our construction will be:

(iv) If $\text{lh}(s) = n + 1$, then $T_s(\bar{R}, P) \models \delta_n(a)$ for some $a \in |\mathcal{M}|$ and $T_s(\bar{R}, P) \models \psi_n$ for some $\psi_n \in \Psi_n$.

Suppose we have constructed all the T_s , $s \in {}^2$, satisfying (i)–(iv). Let η be a fixed element of 2 , $T_\eta =_{\text{df}} \bigcup_{n < \omega} T_{\eta|n}$. T_η satisfies the conditions of 4.3 (especially by (iv)), with $C = |\mathcal{M}|$. Hence, by 4.3, there is a model $\mathcal{M}'_\eta$ of T_η all of whose elements are denoted by some $a \in |\mathcal{M}|$. Since T_η is finitely consistent with $\text{Diag}(\mathcal{M})$ and T_η is complete (cf. 4.3), $\text{Diag}(\mathcal{M}) \subset T_\eta$. It follows that $a \mapsto a^{\mathcal{M}'_\eta}$ is an isomorphism of $\mathcal{M}$ onto $\mathcal{M}'_\eta|L$, hence we can assume that $\mathcal{M}'_\eta|(L \cup \{P\})$ is of the form $(\mathcal{M}, P_\eta)$. It follows from (i) and (ii) that $\{P_\eta : \eta \in {}^2\}$ is a perfect subset of ${}^{|\mathcal{M}|}2$, proving the theorem. What is left is carrying out the construction of the T_s .

Define $M_0 = \emptyset$ and $T_0(\bar{R}, P) = \Psi(\bar{R}, P)$. The essential condition (iii)₀ is satisfied by our hypotheses. Assume next that $T_s(\bar{R}, P)$ has been defined for all s with $\text{lh}(s) = n$ (and so, M_n has been defined as well). To define $T_{s(0)}$ and $T_{s(1)}$, we prove first:

9.4. CLAIM. There are $P_0, P_1 \subset |\mathcal{M}|$, $P_0 \neq P_1$, such that $(\mathcal{M}, a)_{a \in M_n} \models \exists \bar{R} \wedge (T_s(\bar{R}, P_i) \cup \Theta(P_i))$ for $i = 0, 1$.

Otherwise, if this were false, we would have

$$(\mathcal{M}, a)_{a \in M_n} \models \exists P_0 \exists P_1 \exists \bar{R}_0 \exists \bar{R}_1 \wedge S$$

where S is the Σ_A theory of $L(\bar{R}_0, \bar{R}_1, P_0, P_1)_A$ defined by $S = T_s(\bar{R}_0, P_0) \cup \Theta(P_0) \cup T_s(\bar{R}_1, P_1) \cup \Theta(P_1) \cup \{P_0 \neq P_1\}$. Then, since $\mathcal{M}' = (\mathcal{M}, a)_{a \in M_n}$ is Σ -saturated, by relation universality (cf. 7.4) there is an $L(M_n)$ -consequence $\neg \psi$ of S that fails to hold in $\mathcal{M}'$. Thus, $\mathcal{M}' \models \psi$ and $\{\psi\} \cup T_s(\bar{R}_0, P_0) \cup \Theta(P_0) \cup T_s(\bar{R}_1, P_0) \cup \Theta(P_1) \models P_0 = P_1$, i.e., for every $L(M_n)$ -model $\mathcal{N}$ of ψ there is at most one P such that $(\mathcal{N}, P) \models \exists \bar{R} \wedge (T_s(\bar{R}, P) \cup \Theta(P))$. So, by Beth's theorem 8.6, there is an $L(M_n)$ -formula $\theta(v, a)$ such that $\{\psi\} \cup T_s(\bar{R}, P) \cup \Theta(P) \models \forall v (P(v) \leftrightarrow \theta(v, a))$. But then $\{\psi\} \cup T_s(\bar{R}, P) \cup \Theta(P)$ is contradictory (since $\neg \exists u \forall b (P(v) \leftrightarrow \theta(v, u))$ belongs to $\Theta(P)$), contradicting $\mathcal{M}' \models \psi$ and the induction hypothesis (iii)_n. This proves 9.4.

Having shown the Claim, for fixed $s \in {}^2$ pick $P_0, P_1 \subset |\mathcal{M}|$ such that $P_0 \neq P_1$ and $(\mathcal{M}', P_i) \models \exists \bar{R} \wedge (T_s(\bar{R}, P) \cup \Theta(P))$ for $i = 0, 1$. Let $a = a_s \in |\mathcal{M}|$ be such that $a \in P_0$ iff $a \notin P_1$. Assume e.g. that $a \in P_0$ and $a \notin P_1$. Define $T'_{s(0)} = T_s \cup \{P(a)\}$ and $T'_{s(1)} = T_s \cup \{\neg P(a)\}$. Now, also fix $i \in \{0, 1\}$. To define $T_{s(i)}$, pick $\bar{R}$ such that $(\mathcal{M}', \bar{R}, P_i) \models T_s(\bar{R}, P)$ and take $T_{s(i)}(\bar{R}, P) = T'_{s(i)}(\bar{R}, P) \cup \{\delta_n(b), \psi_n\}$ where $b \in |\mathcal{M}|$ and $\psi_n \in \Psi_n$ are

chosen so that $(\mathcal{M}', \bar{R}, P_i) \models \delta_n[b] \wedge \psi_n$. This completes the construction of T_s for each $s' = s\langle i \rangle$ of length $n+1$; notice that $T_{s'}$ contains two more constants from $|\mathcal{M}|$, namely a and b , in addition to those in T_s . We let the finite set $M_{n+1} \subseteq |\mathcal{M}|$ contain M_n and all the a and b involved in the finitely many $T_{s'}$ with $\text{lh}(s') = n+1$. It is clear that our construction will meet the requirements (i)–(iv).

PROOF OF THEOREM 9.1. We have to show the implication (ii) $\Rightarrow$ (iii), i.e., $\neg$ (iii) $\Rightarrow \neg$ (ii). Assuming $\neg$ (iii), the Σ_A -theory $\Psi \cup \Theta(P)$ ($\Theta(P)$ taken from the proof of 9.3) is consistent, hence it has Σ_A -saturated model $(\mathcal{M}, \bar{R}, P_0)$ (cf. 7.3). Then $\mathcal{M}$ is Σ_A -saturated (why?) and P_0 is not L_A -elementary on $\mathcal{M}$. Since $\mathcal{M} \models \sigma$, $\neg$ (ii) is a consequence of 9.3. $\square$

References

- ADDISON, J.
[1962] The theory of hierarchies, in: *Proceedings of the International Congress of Logic, Methodology, and Philosophy of Science*, Stanford, 1960, pp. 26–37.
- BARWISE, J.
[1969] Infinitary logic and admissible sets, *J. Symbolic Logic*, **34**, 226–252.
[1975] *Admissible Sets and Structures* (Springer, Berlin).
- CHANG, C.C.
[1964] Some new results in definability, *Bull. Am. Math. Soc.*, **70**, 808–813.
- CHANG, C.C. and H.J. KEISLER
[1973] *Model Theory* (North-Holland, Amsterdam).
- FRIEDMAN, H.
[1973] Countable models of set theories, in: *Cambridge Summer School in Mathematical Logic*, Lecture Notes in Mathematics, Vol. 337 (Springer, Berlin) pp. 539–573.
- GREGORY, J.
[1973] Uncountable models and infinitary elementary extension, *J. Symbolic Logic*, **38**, 460–470.
- HANF, W.
[1964] Incompactness in languages with infinitely long expressions, *Fund. Math.*, **53**, 309–324.
- HARNIK, V.
[1974] Lecture notes on $L_{\omega_1\omega}$ Dartmouth College, Hanover, NH.
- HARNIK, V. and M. MAKKAÏ
[1976] Applications of Vaught sentences and the covering theorem, *J. Symbolic Logic*, **41**, 171–187.
- HARRISON, J.
[1966] Recursive pseudo-wellorderings, Thesis. Stanford University, Stanford, CA.
- KARP, C.
[1964] *Languages with Expressions of Infinite Length* (North-Holland, Amsterdam).
- KEISLER, H.J.
[1970] Logic with the quantifier “there are uncountably many”, *Ann. Math. Logic*, **1**, 1–93.
[1971] *Model Theory for Infinitary Logic* (North-Holland, Amsterdam).

KLEENE, S.C.

- [1955] Hierarchies of number theoretic predicates, *Bull. Am. Math. Soc.*, **61**, 193–213.

KUEKER, D.

- [1968] Definability, automorphisms, and infinitary languages, in: *The Syntax and Semantics of Infinitary Logic*, edited by J. Barwise, Lecture Notes in Mathematics, Vol. 72 (Springer, Berlin) pp. 152–165.

KRIPKE, S.

- [1964] Transfinite recursion on admissible ordinals, I, II, *J. Symbolic Logic*, **29**, 161–162 (abstract).

LÉVY, A.

- [1965] A hierarchy of formulas in set theory, *Memoirs Am. Math. Soc.*, **57**.

LOPEZ-ESCOBAR, E.G.K.

- [1965] An interpolation theorem for denumerably long sentences, *Fund. Math.*, **57**, 253–272.

MAKKAI, M.

- [1964] On a generalization of a theorem of E.W. Beth, *Acta Math. Acad. Sci. Hungar.*, **15**, 227–235.

- [1973a] Vaught sentences and Lindstrom's regular relations, in: *Cambridge Summer School in Mathematical Logic*, Lecture Notes in Mathematics, Vol. 337 (Springer, Berlin) pp. 622–660.

- [1973b] Global definability theory in $L_{\omega_1, \omega}$, *Bull. Am. Math. Soc.*, **79**, 916–921.

MALITZ, J.

- [1971] Infinitary analogs of theorems from first order model theory, *J. Symbolic Logic*, **36**, 216–228.

MANSFIELD, R.

- [1970] Perfect subsets of definable sets of real numbers, *Pacific J. Math.*, **35**, 451–457.

MOSCHOVAKIS, Y.N.

- [1970] The Suslin–Kleene theorem for countable structures, *Duke Math. J.*, **37**, 341–352.

- [1974] *Elementary Induction on Abstract Structures* (North-Holland, Amsterdam).

PLATEK, R.

- [1966] Foundations of recursion theory, Dissertation and Supplement, Stanford University, Stanford, CA.

RESSAYRE, J.-P.

- [1976] Models with compactness properties relative to an admissible language, *Ann. Math. Logic*, to appear.

REYES, G.

- [1970] Local definability theory, *Ann. Math. Logic*, **1**, 95–137.

SCOTT, D.

- [1964] Invariant Borel sets, *Fund. Math.*, **56**, 117–128.

- [1965] Logic with denumerably long formulas and finite strings of quantifiers, in: *The Theory of Models*, edited by J.W. Addison et al. (North-Holland, Amsterdam; 2nd reprint 1972) pp. 329–341.

SCHLIPF, J.S.

- [1976] A guide to the identification of admissible sets above structures.

SVENONIUS, L.

- [1965] On the denumerable models of theories with extra predicates, in: *The Theory of Models*, edited by J.W. Addison et al. (North-Holland, Amsterdam; 2nd reprint 1972) pp. 376–389.

VAUGHT, R.

- [1973] Descriptive set theory in $L_{\omega_1, \omega}$ in: *Cambridge Summer School in Mathematical Logic*, Lecture Notes in Mathematics, Vol. 337 (Springer, Berlin) pp. 574–598.

- [1974] Invariant sets in topology and logic, *Fund. Math.*, **82**, 269–293.

Doctrines in Categorical Logic

A. KOCK

G. E. REYES

Contents

Preface	284
1. Algebraic theories	284
2. Cartesian theories	289
3. Elementary doctrines: quantifiers as adjoints	293
4. Logical categories: coherent logic	295
5. Grothendieck topoi: infinitary coherent logic	298
6. Elementary topoi	302
7. Topoi and axiomatic set theory	308
8. Other fields of research in categorical logic	310
References	311

Preface

The aim of this paper is to give a survey of category-theoretic methods in logic, in particular in model theory and set theory. We organize the material by increasing richness of the “doctrines” involved. These doctrines are categorical analogues of fragments of logical theories which have sufficient category-theoretic structure for their models to be described as functors. In particular, we deal with the doctrines of equational, cartesian, finitary coherent and infinitary coherent logic. Higher order logic and set theory are touched upon in Sections 6 and 7.

Certain themes run through the various doctrines: invariance of presentation, relative interpretation, completeness, conceptual completeness and generic structures (as well as operations performed on these).

Fundamental to the functorial approach to model theory is the introduction of universes (categories) other than sets where models live. This makes possible the notion of generic structure considered here.

1. Algebraic theories

The introduction of the categorical notion of algebraic theory led to a systematic theory of relative interpretations of one equational theory into another, as well as a theory about the categories (or varieties) of algebras for these, and their relationship. This progress springs from having a presentation-invariant notion of equational (or algebraic) theory.

1.1. HISTORICAL REMARK. It is clear that the two standard ways of presenting the notion of *abelian group*: (i) a set equipped with a binary operation ‘plus’, a unary operation ‘minus’ and a nullary operation (constant) 0 (with certain equations satisfied) — or, (ii) a set equipped with a binary ‘minus’ and a nullary ‘0’ (with certain equations satisfied) — only differ in what operations are considered primitive and which derived. The “equational theories” are the same, or the “totality” of operations (primitive and derived) can be identified in the two cases, and in such a way that the substitution process of operations into other operations are preserved under the identification. To understand this phenomenon in precise terms as an isomorphism between two mathematical structures “consisting of” operations, and equipped with some kind of substitution structure, led to invention of concepts like “Clone of operations” (P. Hall, see COHN [1965]), or “compositeur” (LAZARD [1955]), but these were somewhat

unmanageable notions. The right way of conceiving the totality of operations for an equational theory was found by LAWVERE [1963] who realized that *substitution* should be viewed as the composition of arrows in a certain kind of category:

1.2. DEFINITION. An *algebraic theory* T is a category whose objects are the natural numbers $0, 1, 2, \dots$ and which for each n is equipped with an n -tuple of maps

$$\text{proj} : n \rightarrow 1, \quad i = 1, \dots, n$$

making n into the n -fold categorical product of 1 , $n = 1^n$.

1.3. EXAMPLE. We define an algebraic theory T with

$$\begin{aligned} \text{hom}(n, m) = & m\text{-tuples of polynomials} \\ & \text{in } X_1, \dots, X_n, \text{ with integral coefficients} \end{aligned}$$

with substitution of polynomials as composition. (The proj_i is just X_i , considered as a polynomial in the variables $X_1, \dots, X_n$, $1 \leq i \leq n$.) This T is called the *theory of commutative rings*. For further examples, see 1.14.

1.4. For every algebraic theory, a map $n \rightarrow m$ in it can be described by an m -tuple of maps $n \rightarrow 1$ because m is an m -fold product of 1 ; so the maps $n \rightarrow 1$ play a special role, they are called the *n -ary operations* of the theory. In the example above, an n -ary operation is a polynomial in n variables, which is also precisely what an n -ary (derived) operation is in any presentation of the equational theory of commutative rings.

Similarly, there exist algebraic theories for all other equational theories like the theory of groups, lattices, Lie-algebras, $\dots$; in these, the n -ary operations are (composite) operations in n variables (that is, are *n -ary terms*), with two such identified if their equality follows from the axioms (basic equations) of the theory. This description indicates how one constructs an algebraic theory (in the sense of Definition 1.2) for each equational theory. This might be called the syntactical way of constructing algebraic theories.

The semantics of algebraic theories, that is, the process which leads from the theory to its category of models, can now be explained in the following way.

1.5. DEFINITION. Let T be an algebraic theory, and $\mathcal{E}$ a category with finite products. The *category of T -algebras* or *T -models in $\mathcal{E}$* is the full subcategory

ory $\text{Alg}(\mathcal{T}, \mathcal{E})$ of the functor category $[\mathcal{T}, \mathcal{E}]$ whose objects are the finite product preserving functors.

1.6. REMARK. (i) When considering $\text{Alg}(\mathcal{T}, \mathcal{E})$, we call $\mathcal{E}$ the *value* category. If $\mathcal{E} = (\text{Sets})$, we write $\text{Alg}(\mathcal{T})$ for $\text{Alg}(\mathcal{T}, \mathcal{E})$.

(ii) We know the value of an algebra $A : \mathcal{T} \rightarrow \mathcal{E}$ at an $n \in \mathcal{T}$ if we know $A(1)$, since $A(n) = A(1)^n$, A being product preserving and n being 1^n . To describe A on the morphisms of $\mathcal{T}$, say, a morphism ("operation") $\omega : 2 \rightarrow 1$, amounts to describing a map

$$A(2) = A(1) \times A(1) \xrightarrow{A(\omega)} A(1),$$

that is, a binary operation on the object $A(1)$. So in case $\mathcal{E} = (\text{Sets})$, A interprets abstract binary operations $\omega : 2 \rightarrow 1$ as actual binary operations on a single set $A(1)$, called the *underlying set* of the algebra A .

(iii) With these remarks, it is not hard to understand why, in case, say, where $\mathcal{T}$ is the algebraic theory of commutative rings, we have an equivalence of categories $\text{Alg}(\mathcal{T}, (\text{Sets})) \simeq \text{Category of commutative rings}$. One should note that the naturality requirement on transformations $\tau : A \rightarrow B$ precisely amounts to requiring that $\tau_1 : A(1) \rightarrow B(1)$ is a homomorphism with respect to all the operations of the theory. If, for instance, $\omega : 2 \rightarrow 1$ is a binary operation in $\mathcal{T}$, both things amount to commutativity of the diagram

$$\begin{array}{ccccc} A(1) \times A(1) & \simeq & A(2) & \xrightarrow{\omega_A} & A(1) \\ \tau_1 \times \tau_1 \downarrow & & \downarrow \tau_2 & & \downarrow \tau_1 \\ B(1) \times B(1) & \simeq & B(2) & \xrightarrow{\omega_B} & B(1) \end{array}$$

(the left-hand square being also commutative because of naturality).

1.7. Relative interpretation

As mentioned, relative interpretations of one equational theory into another can now be dealt with very rationally:

1.8. DEFINITION. A *morphism* of algebraic theories is a functor $f : \mathcal{T} \rightarrow \mathcal{T}'$ with $f(n) = n$ and with $f(\text{proj}_i) = \text{proj}_i'$ for all the specified projections.

1.9. EXAMPLE. We give two trivial and one non-trivial example.

(i) Let $\mathcal{T}$ be the theory of abelian groups, $\mathcal{T}'$ the theory of commutative rings. There is an obvious inclusion $\mathcal{T} \rightarrow \mathcal{T}'$, in fact $\mathcal{T}(n, 1)$ may be viewed as

the subset of $T'(n, 1)$ (= set of polynomials in n variables) consisting of homogeneous degree 1 polynomials.

(ii) Let T be the theory of groups, T' the theory of abelian groups. There is an obvious 'surjective' $T \rightarrow T'$ obtained by identifying two abstract group operations if their equality follows from the commutative law. Studying the quotients of a theory T in fact is equivalent to studying the subvarieties of the variety it defines, to express things in Birkhoff terms (COHN [1965]).

(iii) Let T be the theory of Lie-rings, T' the theory of (associative but not necessarily commutative) rings. There is a morphism $T \rightarrow T'$ which sends the binary $[-, -]$ in T into the commutator operation ω in T' , $\omega(x, y) = x \cdot y - y \cdot x$.

1.10. If $f : T \rightarrow T'$ is a morphism of algebraic theories, one immediately gets a functor "composing with f "

$$f^b : \text{Alg}(T', \mathcal{E}) \rightarrow \text{Alg}(T, \mathcal{E}).$$

This feature is common to all kinds of functorial semantics. In the case of algebraic theories (next section), one can say more, namely (LAWVERE [1963]):

1.11. THEOREM. *If the value category $\mathcal{E}$ is (Sets) (or any other locally presentable category, GABRIEL and ULMER [1971]), the functor f^b has a left adjoint.*

PROOF. For a proof in the (Sets) case we refer to SCHUBERT [1970]. $\square$

1.12. Free algebras

The existence of such can be considered as a corollary of Theorem 1.11, by taking the T in 1.10 to be the algebraic theory whose *only* n -ary operations are the projections, and whose category of algebras is just (Sets). The functor f^b can be identified with $A \mapsto A(1)$, which is a functor $\text{Alg}(T') \rightarrow (\text{Sets})$. It has a left adjoint $F : (\text{Sets}) \rightarrow \text{Alg}(T')$, by 1.11. An algebra of form $F(M)$ (M a set) is called the *free* algebra on the set M of generators. It now turns out that any algebraic theory can be reconstructed from the free algebras:

1.13. THEOREM. *Let T be an algebraic theory. Then T is equivalent to the dual of the full subcategory of $\text{Alg}(T)$ defined by the free algebras $F(n)$ ($n = 0, 1, 2, \dots$).*

PROOF. The functor $\text{hom}_T(n, -) : T \rightarrow (\text{Sets})$ preserves products and is thus a T -algebra. For any other T -algebra $A : T \rightarrow (\text{Sets})$, we have (denoting by Hom the hom-functor of $[T, (\text{Sets})]$ and thus of $\text{Alg}(T)$):

$$\text{Hom}(\text{hom}_T(n, -), A) \simeq A(n) \simeq \prod_n A(1) \simeq \text{hom}(n, A(1)),$$

the first isomorphism by Yoneda's lemma. Thus $\text{hom}_T(n, -)$ serves as $F(n)$. The second conclusion is now immediate, again by Yoneda. $\square$

1.14. EXAMPLE. The following is an example of an algebraic theory which is neither obtained by a presentation, nor by "semantic" means as in 1.13, but rather by a construction performed in the *category* of algebraic theories. Let $\hat{T}_0$ be the theory whose n -ary operations are formal power series in n variables and without constant term. They can be substituted into each other without any convergence trouble, since the constant term is missing. Formally, $\hat{T}_0$ can be obtained as an inverse limit formation in the category of algebraic theories, $\varprojlim T_{0,n}$, where $T_{0,n}$ is the algebraic theory for commutative rings without unit and satisfying $\forall x: x^n = 0$. The algebras for $\hat{T}_0$ are not known, neither is a syntactic presentation.

1.15. Varying the value category

We can consider $\text{Alg}(T, \mathcal{E})$ for *any* category $\mathcal{E}$ with finite products; in particular when $\mathcal{E} = (\text{Alg}(T'))^{\text{op}}$. In this case one gets the notion of " T -coalgebra in the category of T' -algebras", see Wraith [1969] and Freyd [1966], which covers structures like Hopf algebras which cannot be described in terms of classical universal algebra (not even in finitary first-order logic).

1.16. The generic algebra

It is clear that if $p : \mathcal{E} \rightarrow \mathcal{E}'$ is a product preserving functor, we get a functor 'transport along p '

$$\text{Alg}(T, \mathcal{E}) \rightarrow \text{Alg}(T, \mathcal{E}')$$

by composing with p . We give a trivial example of this, which, however, is a case of an important principle which we shall meet in Sections 2, 4 and 5, the principle of *generic structure*. For a given algebraic theory T , we may consider $\text{Alg}(T, T)$, which makes sense since T has finite products. Among the T -algebras in T , we have the identity functor $\text{id}_T : T \rightarrow T$. It is a *generic* T -algebra in the sense that any other T -algebra $A : T \rightarrow \mathcal{E}$ in any category $\mathcal{E}$ (with finite products) can be obtained by transport of the algebra id_T along

the product preserving functor A (clearly, since $A \circ \text{id}_T = A$). (The example 1.9(iii) can be seen in this light: we equip (the underlying object 1 of) the generic associative T' -algebra (associative ring) with the structure of a Lie ring.)

However, the category T in which the generic T -algebra lives, is rather poor in categorical structure. In the next section, we shall encounter a richer category $\text{FP}(T)^{\text{op}}$ in which also lives a generic T -algebra (this time for cartesian (= finite limit preserving) functors) — and similarly for each of the stronger doctrines we meet later. The richer contexts make certain constructions on T -algebras possible ‘once and for all’, namely as constructions on the generic T -algebra.

1.17. Limitations

It is possible to characterize in categorical terms categories which come about as $\text{Alg}(T)$ for some algebraic theory T , see LAWVERE [1965a]. Some that do not are the category Cat of small categories, the category of algebraic theories, or the category of partially ordered sets. These can be dealt with in terms of functorial semantics using a somewhat richer notion of “theory”: a small cartesian category. This kind of functorial semantics is what GABRIEL and ULMER [1971] is about. We shall motivate cartesian theories by an example of a relative interpretation of one theory into another which cannot be described in the framework of algebraic theories.

2. Cartesian theories

2.1. EXAMPLE (Descartes, roughly). Consider the functor “circle”

$$S^1: (\text{Commutative rings}) \rightarrow (\text{Sets})$$

which to a ring A associates the set $S^1(A)$,

$$S^1(A) = \{(x, y) \in A^2 \mid x^2 + y^2 = 1\}.$$

This set even carries an abelian group structure defined as follows:

$$(x, y) \cdot (x', y') = (x \cdot x' - y \cdot y', x \cdot y' + y \cdot x')$$

(Gauss) Denoting by T and T' the algebraic theories of commutative rings and abelian groups, respectively, we thus have a functor

$$S^1: \text{Alg}(T) \rightarrow \text{Alg}(T'). \quad (2.1)$$

If $\mathcal{C}$ is a cartesian category (= having finite inverse limits), it has

equalizers, and if $A : \mathcal{T} \rightarrow \mathcal{E}$ is a commutative ring object, we can use the equalizer of

$$A(X_1^2 + X_2^2) \quad \text{and} \quad A(1) \quad (2.2)$$

(both the arguments of A being viewed as morphisms $2 \rightarrow 1$ in $\mathcal{T}$) to define S^1 . In this way, the context of (2.1) is extended so as to define a functor

$$S^1 : \text{Alg}(\mathcal{T}, \mathcal{E}) \rightarrow \text{Alg}(\mathcal{T}, \mathcal{E})$$

for any *cartesian* category $\mathcal{E}$.

Unlike the functor (Associative algebras) $\rightarrow$ (Lie algebras) considered in 1.9(iii), the functor S^1 is not describable by performing the S^1 -construction once and for all on the 'generic commutative ring' in $\mathcal{T}$, because $\mathcal{T}$ does not possess the requisite equalizer. This motivates looking for a notion of *cartesian* theory where such constructions can be performed, and investigating the functorial semantics of such:

2.2. DEFINITION. A *cartesian theory* $\mathbf{C}$ is a small category with finite inverse limits. A *model* M for $\mathbf{C}$ with *values* in a category $\mathcal{E}$ with finite inverse limits is a functor $M : \mathbf{C} \rightarrow \mathcal{E}$ which preserves these limits; a *morphism* of models, $M \rightarrow M'$ is any natural transformation from M to M' .

2.3. REMARK. Thus we have defined a *category* of models with values in $\mathcal{E}$, frequently denoted $\text{Lex}(\mathbf{C}, \mathcal{E})$ since its objects are the left exact (= finite inverse limit preserving = cartesian) functors. It depends functorially on both $\mathbf{C}$ and $\mathcal{E}$: any left exact functor $\mathcal{E} \rightarrow \mathcal{E}'$ between the value categories defines a 'transport' functor between the model categories, $\text{Lex}(\mathbf{C}, \mathcal{E}) \rightarrow \text{Lex}(\mathbf{C}, \mathcal{E}')$. Any left exact functor $\mathbf{C} \rightarrow \mathbf{C}'$ between cartesian theories ('relative interpretation') induces a functor $\text{Lex}(\mathbf{C}, \mathcal{E}) \rightarrow \text{Lex}(\mathbf{C}', \mathcal{E})$ between the model categories. As in the case of algebraic theories, such functors have left adjoints provided $\mathcal{E} = (\text{Sets})$ (or any other locally presentable category). The reader may find a thorough treatment of categorical properties of categories of this form in GABRIEL and ULMER [1971] (in their notation, $\text{Lex}(\mathbf{C}, \mathcal{E}) = \text{St}_\alpha(\mathbf{C}, \mathcal{E})$ with $\alpha = \aleph_0$). Among the theorems in their book is one which we would term a (strong form) of conceptual completeness of cartesian theories:

2.4. THEOREM. Suppose $\mathbf{C}$ and $\mathbf{C}'$ are cartesian theories such that $\text{Lex}(\mathbf{C}, (\text{Sets})) \simeq \text{Lex}(\mathbf{C}', (\text{Sets}))$. Then $\mathbf{C} \simeq \mathbf{C}'$.

PROOF. The proof follows from the fact that $\mathbf{C}$ can be reconstructed from

$\text{Lex}(\mathbf{C}, (\text{Sets}))$ as the dual of the subcategory of (abstractly) finitely presentable objects (GABRIEL and ULMER [1971], §7, in particular 7.10). $\square$

2.5. Comparison with algebraic theories

The clue to the proof that the doctrine of cartesian theories comprises that of algebraic theories also lies in the notion of finitely presented object. In a category of form $\text{Alg}(\mathbf{T})$, the finitely presented objects form precisely the smallest subcategory containing all objects of form $F(n)$, and stable under finite colimits. Every finitely presented algebra A can be described as a coequalizer in $\text{Alg}(\mathbf{T})$,

$$F(n') \rightrightarrows F(n) \rightarrow A,$$

(and a finite colimit of finitely presented algebras is finitely presented). We denote this subcategory $\text{FP}(\mathbf{T})$. If α is a functor from the full subcategory of $\text{Alg}(\mathbf{T})$ consisting of the objects of form $F(n)$ ($n = 0, 1, \dots$) (and which we may identify with $\mathbf{T}^{\text{op}}$, by 1.13) into a category with finite colimits, then it extends, because of the above coequalizer, in at most one way to a finite colimit preserving functor on $\text{FP}(\mathbf{T})$, and a necessary condition that it does, is, of course, that α preserves finite coproducts (since $F(n) + F(m) = F(n + m)$). This necessary condition is also sufficient: we formulate this in the following theorem, where we, however, first change the variance.

2.6. THEOREM. *Let $A : \mathbf{T} \rightarrow \mathcal{E}$ be a finite product preserving functor from an algebraic theory into a cartesian category (so A is an algebra for $\mathbf{T}$). Then the following diagram can be filled in with a left exact functor $\bar{A}$ (which is uniquely determined up to isomorphism):*

$$\begin{array}{ccc} \mathbf{T} & \xrightarrow{\quad} & \text{FP}(\mathbf{T})^{\text{op}} \\ \bar{A} \searrow & & \swarrow \bar{A} \\ & \mathcal{E} & \end{array}$$

(The top functor being $n \mapsto F(n)$ as studied also in 1.13.)

PROOF. For the case $\mathcal{E} = (\text{Sets})$, it follows because $\text{Alg}(\mathbf{T})$ is locally finitely presentable, thus can be reconstructed as the category of set-valued left exact functors on the dual of the category of finitely presented objects in it (GABRIEL and ULMER [1971], 7.9). It now easily follows also for $\mathcal{E}$ a functor category $[\mathbf{C}^{\text{op}}, (\text{Sets})]$. Further, if the values of A are representable functors the values of $\bar{A}$ will be finite inverse limits of representables, and

will themselves be representable, provided $\mathbf{C}$ has finite inverse limits. This proves the theorem for $\mathcal{E} = \mathbf{C}$. $\square$

2.7. REMARK. The way to read the theorem (provided the value category has finite inverse limits) is: Every category of algebras for an algebraic theory $\mathbf{T}$ can be considered the category of models for a cartesian theory $\mathbf{P} = \mathbf{FP}(\mathbf{T})^{\text{op}}$. The identification identifies $\mathbf{A}$ with $\bar{\mathbf{A}}$ in the above diagram.

2.8. Scope of the doctrine

As mentioned in 1.17, there are notions, like ‘partially ordered set’, which can be expressed by functorial semantics of a cartesian theory but not of an algebraic theory. (The appropriate cartesian theory $\mathbf{C}$ is in this case the dual of the category of finite partially ordered sets). How this works in detail can be seen in GABRIEL and ULMER [1971], 8.2b, or in the work of the Ehresmann school, where one may find many examples of cartesian theories or the closely related ‘esquisses’, see BASTIANI and EHRESMANN [1972].

2.9. Syntactic characterization of the doctrine

A sufficient condition for a first order theory to have its category of models (where maps are those that preserve the primitive predicates and operations) of the form $\text{Lex}(\mathbf{C}, (\text{Sets}))$ for a suitable cartesian theory $\mathbf{C}$, is that the axioms of the theory are simple Horn sentences, that is, of form

$$\forall \mathbf{x} (\varphi(\mathbf{x}) \Rightarrow \exists ! \mathbf{y} \psi(\mathbf{x}, \mathbf{y}))$$

($\mathbf{x}$ and $\mathbf{y}$ are tuples of variables) with φ and ψ conjunctions of atomic formulae — see KEANE [1975]. The theory may be allowed to be many sorted; this corresponds to the fact that a cartesian theory $\mathbf{C}$ unlike an algebraic theory $\mathbf{T}$ does not have a preferred ground object. — There is a sense in which Keane’s condition also goes the other way, but it is not clear to us.

2.10. EXAMPLE (continuation of 2.1). The functor (2.1) is not induced by a morphism of algebraic theories. However, if we take the corresponding cartesian theories, it is. Equivalently, out of the generic ring object in the cartesian theory $\mathbf{C}$ of commutative rings, we can construct the circle object (and its group structure), once and for all, that is, we have a *generic circle*. If A^1 denotes the generic ring object in $\mathbf{C}$, the generic S^1 is constructed as the equalizer in $\mathbf{C}$

$$S^1 \rightarrow A^2 \rightrightarrows A^1$$

where the two displayed maps from $A^2 (= A^1 \times A^1)$ to A^1 are the ring operations $X_1^2 + X_2^2$ and 1 , applied on the ring object A^1 . Now, recalling that $\mathbf{C} = (\text{finitely presented commutative rings})^{\text{op}}$, and $A^1 = F(1)$, $A^2 = F(2)$, we see that S^1 is the finitely presented commutative ring which is the coequalizer

$$S^1 \leftarrow Z[X_1, X_2] = F(2) \rightleftarrows Z[X] = F(1)$$

(the two parallel maps again being given by $X \mapsto X_1^2 + X_2^2$ and $X \mapsto 1$, respectively). So

$$S^1 = Z[X_1, X_2]/(X_1^2 + X_2^2 - 1).$$

The group structure on S^1 , when viewed in $\mathbf{C}$, is a co-group structure (1.15) when viewed in the dual more familiar category, the category of finitely presented commutative rings. As such, it is a map $S^1 \rightarrow S^1 \otimes S^1$ (which cannot be described in first-order terms). — This way of thinking on the circle, and other ‘algebraic subsets’ or ‘affine schemes’ in affine space A^n , is familiar in modern algebraic geometry, see e.g. DEMAZURE and GABRIEL [1970].

3. Elementary doctrines: quantifiers as adjoints

3.1. Once equational and cartesian logic have been set in a categorical context, it is natural to search for a categorical description of the logic of quantifiers. The basic observation, due to LAWVERE [1965b], [1969] and [1970], is that existential and universal quantification can be seen as left and right adjoints, respectively, of substitution. Lawvere used this description as basis for arriving at a functorial semantics of first-order logic, first in the context of ‘elementary theories’, see LAWVERE [1965b], further developed by VOLGER [1975], and later in the context of ‘hyperdoctrines’ and ‘elementary existential doctrines’, LAWVERE [1970], p. 6. We shall discuss the latter.

3.2. DEFINITION. An *elementary existential doctrine* (*eed*) is given by a base category $\mathbf{T}$ with finite products (whose objects and morphisms one should think of as the *types* and *terms*, respectively), and for each object (type) n , there is given a category $B(n)$, the “category of *attributes*” of that type. (For applications in logic, the attribute category is usually, but not always, just a partially ordered set, the order relation being thought of as entailment.) The basic structure required is now that $B(n)$ depends

contravariantly functorial on n , that is, for $f : n \rightarrow m$ a morphism in $\mathbf{T}$, there is given a functor (= order preserving map) $B(f) : B(m) \rightarrow B(n)$, thought of as substitution along f , and having a left adjoint $\exists_f$, “existential quantification along f ”.

3.3. REMARK. In Lawvere’s original treatment of eed’s, $B(n)$ is assumed to be a cartesian closed category, but there are as many variants of the notion as there are fragments of first-order language (roughly).

3.4. EXAMPLE. Any category $\mathcal{E}$ with finite inverse limits and good direct images defines an eed $P(\mathcal{E})$ with $\mathbf{T} = \mathcal{E}$, $B(n) =$ subobject semilattice of $n \in \mathcal{E}$, and $B(f) =$ inverse image formation (pull-back) along f . The $B(n)$ ’s will have, and the $B(f)$ ’s preserve, more or less lattice theoretic properties, depending on the exactness properties of $\mathcal{E}$, leading to the variants of the doctrine notion. We shall discuss the applicability of eed’s for functorial semantics by considering the boolean case, where we have an (abstract) eed where each $B(n)$ is a boolean algebra, and each $B(f)$ a boolean homomorphism, and by considering only (Sets) as value category; note that $P((\text{Sets}))$ is a boolean eed. Thus:

3.5. DEFINITION. A (set-valued) *model* of the boolean eed $(\mathbf{T}, B)$ is a morphism of boolean eed’s

$$(\mathbf{T}, B) \rightarrow P((\text{Sets})),$$

(where a morphism of boolean eed’s $(\mathbf{T}, B) \rightarrow (\mathbf{T}', B')$ is a product preserving functor $M : \mathbf{T} \rightarrow \mathbf{T}'$ between the base categories, as well as, for each $n \in \mathbf{T}$, a boolean homomorphism $B(n) \rightarrow B'(M(n))$, satisfying obvious compatibility conditions).

3.6. To relate this notion of model to the notion of model for an ordinary first-order theory $\mathcal{T}$, one has to take $(\mathbf{T}, B)$ to be the ‘Lindenbaum doctrine’ of $\mathcal{T}$, where $\mathbf{T}$ is the algebraic theory having no other operations than the projectors (as studied in 1.12) and with $B(n) = \mathcal{T}$ -equivalence classes of formulas whose free variables are among $x_1, \dots, x_n$. Then $B(f)$ (for $f : n \rightarrow m$) is defined by means of the syntactic process of substitution. Existential quantification can be defined in terms of the syntactic $\exists$. Sketches of this kind of semantics for eed’s are given in LAWVERE [1970] (for the higher order case); see also COSTE [1973].

The reader familiar with polyadic or cylindric algebras may recognize features in the (boolean) eed-approach, and in fact, specific comparison theorems have been proved, JOYAL [1971].

3.7. However, from the viewpoint of categories as theories, eed's have the defect that they are categories $\mathcal{T}$ equipped with something extra, the $B(n)$'s, which is not defined in terms of the category structure, except for the case of a subobject eed $P(\mathcal{E})$ (Example 3.4). For which eed's $(\mathcal{T}, B)$, or for which first-order theories $\mathcal{T}$ does there exist a sufficiently rich cartesian category $\mathbf{R}$ such that $(\mathcal{T}, B)$ (or $\mathcal{T}$) has the same models as the subobject eed $P(\mathbf{R})$? Equivalently, when can the $\mathcal{E}$ -valued models of $(\mathcal{T}, B)$ (or $\mathcal{T}$) be described as functors $\mathbf{R} \rightarrow \mathcal{E}$ preserving a certain amount of the categorical structure? This question was first resolved by Joyal-Reyes-Dionne (DIONNE [1973] for some of the fragments); see Example 4.4. Dionne's method was to construct $\mathbf{R}$ from $\mathcal{T}$. Better proofs of these results have been given by Benabou-Coste (COSTE [1974]) who construct actual 'good' categories $\mathbf{R}$ from eed's satisfying the 'Beck' (or Chevalley) and 'Frobenius' laws (terminology of LAWVERE [1970]), and apply this construction to the Lindenbaum doctrine of $\mathcal{T}$ (for the appropriate fragment of logic). Another technique is due to Freyd via the notion of allegory, a categorical axiomatization of the relation calculus.

4. Logical categories: coherent logic

The search for categorical versions of first-order logic in the spirit of equation theories with categories and models with functors led to the notion of regular category with stable sups, or logical category, for short, of Joyal-Reyes, REYES [1974]. (As pointed out in Section 3, Lawvere and Volger had studied earlier the related notion of "elementary theory" and "elementary doctrine".) In the context of logical categories, existential quantifiers appear as images (in the categorical sense) of the connective $\vee$ ("or") as a supremum (of subobjects), whereas $\wedge$ ("and") and substitution (of variables by terms) are cases of inverse limits.

4.1. DEFINITION. A *logical category* $\mathcal{T}$ is a cartesian category with

- (a) images which are stable under pull-backs,
- (b) finite sups of subobjects of a given object which are stable under pull-backs.

4.2. REMARK. (ad (a)) The image of $f : A \rightarrow B$ is the smallest subobject $I \rightarrow B$ through which f factors. We write $f : A \twoheadrightarrow B$ to mean that the image of f is B itself.

We say that $f : A \twoheadrightarrow B$ is stable, if for every pull-back diagram

$$\begin{array}{ccc}
 A & \xrightarrow{f} & B \\
 \uparrow & & \uparrow \\
 A' & \xrightarrow{f'} & B'
 \end{array}$$

the image of f' is B' .

(ad (b)) We say that $\bigvee_{i \in I} A_i = A$ is stable if for every $B \rightarrow A$,

$$\bigvee_{i \in I} B_A \times A_i \simeq B.$$

4.3. DEFINITION. A *logical morphism* between logical categories $f: \mathcal{T} \rightarrow \mathcal{T}'$ is a functor which preserves finite inverse limits, images and finite sups.

We let $\text{Mod}_{\mathcal{T}}(\mathcal{T})$ be the full subcategory of the functor category $[\mathcal{T}, \mathcal{T}']$ consisting of logical morphisms. In the particular case $\mathcal{T}' = (\text{Sets})$, the morphisms are called models of $\mathcal{T}$ and we define $\text{Mod}(\mathcal{T}) = \text{Mod}_{(\text{Sets})}(\mathcal{T})$.

4.4. EXAMPLE. Joyal–Reyes–Dionne (DIONNE [1973]) proved that those first-order theories whose categories of models (with primitive-predicate preserving maps as morphisms) are of the form $\text{Mod}_{(\text{Sets})}(\mathcal{T})$ are precisely the *coherent* theories $\mathcal{T}$, as defined by Joyal–Reyes, in REYES [1974]; a first-order theory is *coherent* if it can be presented with axioms of the form

$$\forall x (\varphi(x) \Rightarrow \psi(x))$$

where φ and ψ are built from the atomic formulas by means of $\wedge$, $\vee$ and $\exists$, or are $\uparrow$ or $\downarrow$ ('true' or 'false'). The notion of coherent theory will be crucial in Section 5. The hard part of the proof consists in construction of a logical category $\mathcal{R}$ starting from $\mathcal{T}$. Basically, there is one object for each concept definable in $\mathcal{T}$, and a map for each provably functional relation.

4.5. EXAMPLE. The theory of commutative local rings is coherent, being axiomatizable by equations, and the two axioms

- (i) $\forall x (\uparrow \Rightarrow (\exists y: x \cdot y = 1 \vee \exists y: (x - 1) \cdot y = 1)),$
 (ii) $(1 = 0 \Rightarrow \downarrow).$

(The equations are of the required form again by using $\uparrow$.)

4.6. COMPLETENESS THEOREM (Deligne, GROTHENDIECK [1963–1972], Exposé 6; Joyal). *If $\mathcal{T}$ is a logical category and $f, g: X \rightrightarrows Y$ are two different morphism in $\mathcal{T}$, then there is a model M of $\mathcal{T}$ such that $M(f) \neq M(g)$.*

PROOF (outline). The key idea is to extend $\mathbf{T}$ to a new logical category $\mathbf{T}'$ having the property that every $A \twoheadrightarrow 1$ has a section (i.e. $\mathbf{T}$ satisfies a weak axiom of choice). The key observation in Joyal's proof is the following: whenever $A \twoheadrightarrow 1$ in $\mathbf{T}$ is given, we can add "universally" a formal section by "changing base", i.e., by considering the category $\mathbf{T}/A$ whose objects are morphisms $B \rightarrow A$ and whose morphisms are commutative triangles

$$\begin{array}{ccc} B & \longrightarrow & C \\ & \searrow & \swarrow \\ & A & \end{array}$$

which is again a logical category. The pullback functor $\mathbf{T} \rightarrow \mathbf{T}/A$ (which sends B into $\pi_2: B \times A \rightarrow A$) is conservative and, furthermore $A \twoheadrightarrow 1 \in \mathbf{T}$ has the diagonal $\Delta_A: A \rightarrow A \times A$ as a section in $\mathbf{T}/A$.

By identifying objects with formulas (as in the example) we recognize the analogue of a key step in Henkin's proof: if A is a formula such that $T \vdash \exists x A$, then $T \cup A(a)$ is a conservative extension of T , where a is a new constant.

The rest of the proof proceeds by taking an appropriate ultrafilter. $\square$

4.7. REMARK. One important question that can be asked in the categorical context is: to what extent does the category of models of $\mathbf{T}$ determine $\mathbf{T}$? One way of interpreting this question is to ask whether further logical structure may be introduced in $\mathbf{T}$ without changing the category of models of $\mathbf{T}$ or whether $\mathbf{T}$ is "conceptually complete". We notice at once that logical categories are not "conceptually complete" in general. Indeed, by adding "formally" to $\mathbf{T}$ coproducts and quotients by equivalence relations we obtain a logical category $\hat{\mathbf{T}}$ such that the logical inclusion $\mathbf{T} \rightarrow \hat{\mathbf{T}}$ induces (via composition) an equivalence $\text{Mod}(\hat{\mathbf{T}}) \xrightarrow{\sim} \text{Mod}(\mathbf{T})$ (see ANTONIUS [1975]). (Clearly, e.g. X/R is uniquely interpreted in (Sets) as the quotient of the interpretation of X by that of R .) We find here a *defect* in the usual formalizations of many-sorted languages where the "implicitly definable" operations of coproducts and quotients are not explicit. Letting a *pretopos* be a logical category with "good" coproducts and quotients by equivalence relations, we have:

4.8. CONCEPTUAL COMPLETENESS (MAKKAI and REYES [1976]). *If a logical functor $f: \mathbf{T} \rightarrow \mathbf{T}'$ between pretopoi induces (via composition) an equivalence $\text{Mod } \mathbf{T}' \xrightarrow{\sim} \text{Mod } \mathbf{T}$, then f is an equivalence.*

PROOF. The proof proceeds by introducing syntactical many-sorted presentations for $\mathbf{T}, \mathbf{T}'$ whereby f becomes an interpretation of theories.

Compactness and the method of diagrams are then used. A purely categorical proof is still lacking. $\square$

4.9. REMARK. Infinitary logical categories have also been considered and BARR [1974] has proved a completeness theorem for Boolean-valued models. A Gentzen-type axiomatization for this infinitary coherent logic, with applications to completeness theorems (including Barr's) may be found in MAKKAÏ and REYES [1976].

5. Grothendieck topoi: infinitary coherent logic

Topoi (and pretopoi) appeared in algebraic geometry, where they are ubiquitous via a generalization of the notion of sheaf over a topological space: this is the notion of sheaf over a site, due to Grothendieck.

5.1. DEFINITION. (i) A *site* is a cartesian category $\mathcal{C}$ together with a notion of localization, i.e. for every $A \in |\mathcal{C}|$ we are given a non-empty class $\text{Loc}(A)$ of families of morphisms $(A_i \rightarrow A)_{i \in I}$ of $\mathcal{C}$, called the *localizations* of A which are stable under pullbacks in the sense that for every $B \rightarrow A$, the family $(A_{i_A} \times B \rightarrow B)_{i \in I}$ is a localization of B .

(ii) A *sheaf* over $\mathcal{C}$ is a functor $F : \mathcal{C}^{\text{opp}} \rightarrow (\text{sets})$ satisfying the following conditions, for every $(f_i : A_i \rightarrow A)_{i \in I} \in \text{Loc}(A)$:

- (a) if $\xi, \eta \in F(A)$ are such that $\xi_i = F(f_i)(\xi) = F(f_i)(\eta) = \eta_i$ for all $i \in I$, then $\xi = \eta$.
- (b) if $(\xi_i)_{i \in I}$ is a family such that $\xi_i \in F(A_i)$ for all $i \in I$ and is compatible, i.e. in the diagram

$$\xi_i \in F(A_i) \xrightarrow{F(\pi_i)} F(A_{i_A} \times A_j) \xleftarrow{F(\pi_j)} F(A_j) \ni \xi_j$$

obtained via F from

$$A_i \xleftarrow{\pi_i} A_{i_A} \times A_j \xrightarrow{\pi_j} A_j$$

we have $F(\pi_i)(\xi_i) = F(\pi_j)(\xi_j)$ for all $i, j \in I$, then there is $\xi \in F(A)$ such that $\xi_i = F(f_i)(\xi)$, for all $i \in I$.

We let $\text{Sh}(\mathcal{C})$ be the full subcategory of the functor category $[\mathcal{C}^{\text{op}}, (\text{Sets})]$ consisting of sheaves over $\mathcal{C}$.

(iii) A *Grothendieck topos* is a category equivalent to one of the form $\text{Sh}(\mathcal{C})$, for a small site $\mathcal{C}$.

5.2. REMARK. (i) These notions allow us to give a meaning to the intuitive idea that some concepts, e.g. “real-valued continuous functions with open domain” are of local character. In this example, we identify this concept with the functor $C_R: \text{Open}(X)^{\text{op}} \rightarrow (\text{Sets})$ which to every open set $U \in \text{Open}(X)$ associates its “extension” $C_R(U) = \{f: U \rightarrow \mathbb{R} \mid f \text{ is continuous}\}$. The ordered category $\text{Open}(X)$ may be considered as a site, by defining a localization of U as an open cover of U .

The local character of the concept in question are just the statements (a) and (b).

(ii) A site structure and the corresponding notion of sheaf may be defined on a category $\mathcal{C}$, even if $\mathcal{C}$ does not have finite inverse limits. The definition is technically more involved. Examples of this type appear in model theory (see 5.3(ii)).

(iii) One of the main theorems of topos theory is Giraud’s (GROTHENDIECK [1963–1972], Exposé 4) which characterizes a topos as an ∞ -pretopos with a set of generators (where an ∞ -pretopos is a category with finite inverse limits, “good” infinite coproducts and quotients by equivalence relations). In particular, any topos has a *canonical* site structure given by $(A_i \rightarrow A)_{i \in I}$ is a localization iff the unique map

$$\frac{|\cdot|}{i \in I} A_i \rightarrow A$$

is epimorphic. (“Goodness” is precisely the condition that this type of families are localizations.) This is sometimes called the arbitrary cover localization.

5.3. EXAMPLE. (i) Let B be a complete Boolean algebra, considered as a category. We define the canonical localization as follows: $(a_i)_{i \in I}$ covers a iff $a = \bigvee_{i \in I} a_i$.

Then $\text{Sh}(B)$ is equivalent to the category of Boolean-valued sets and Boolean-valued maps of Scott–Solovay’s universe $V^{(B)}$.

This example opens the way for a category-theoretic approach to independence results in set theory: see HIGGS [1976], TIERNEY [1972], BOILEAU [1975], and BUNGE [1974].

(ii) Let C be a small category. There is a so-called $\neg\neg$ -localization on it which can be described as follows: a family $\{C_i \rightarrow C \mid i \in I\}$ is a $\neg\neg$ -localization if for each $B \rightarrow C$ there is an $A \rightarrow B$ such that for some $i \in I$ we have a commutative diagram

$$\begin{array}{ccc} C_i & \longrightarrow & C \\ \uparrow & & \uparrow \\ A & \longrightarrow & B. \end{array}$$

This $\neg\neg$ -localization will be used below.

(iii) Let $\mathbf{R}$ be a logical category. We introduce a site structure on $\mathbf{R}$, the *finite cover localization*, by defining for I finite:

$$(A_i \xrightarrow{f_i} A)_{i \in I} \in \text{Loc}(A) \quad \text{iff} \quad A = \bigvee_{i \in I} \text{Image}(f_i).$$

The stability conditions on $\mathbf{R}$ guarantee that this is a localization.

5.4. DEFINITION. (i) A functor $F: \mathcal{C} \rightarrow \mathcal{D}$ between two sites is a *site morphism* if it preserves the finite inverse limits and takes localizations of $\mathcal{C}$ into localizations of $\mathcal{D}$. We let $\text{Cont}(\mathcal{C}, \mathcal{D})$ be the full subcategory of the functor category $[\mathcal{C}, \mathcal{D}]$ consisting of site morphisms.

(ii) A *geometric morphism* $p: \mathcal{E} \rightarrow \mathcal{E}'$ between topoi is a couple (p^*, p_*) , where $p^*: \mathcal{E}' \rightarrow \mathcal{E}$ is a left exact functor having p_* as a right adjoint (thus p^* is a site morphism for the canonical site structures on $\mathcal{E}$ and $\mathcal{E}'$).

Remark. The significance of coherent logic lies in the fact that its logical operations (i.e., $\exists, \vee, \wedge, \uparrow, \downarrow$) are preserved by the functor p^* for a geometric morphism p . See also 6.13.

5.5. Forcing: the Kripke–Joyal semantics

From the examples it should be clear that topoi have something to do with forcing and generic structures. A. Joyal pointed out that the various notions of forcing (Cohen’s, Robinson’s, Kripke’s) are special cases of forcing with a site of conditions. Even for a site $\text{Open } X$ (Example 5.2(i)) the usual definitions break down: in Kripke’s semantics, for instance, the validity of a disjunction or existential formula at the “stage” or “time” α are decided “on the spot”, i.e. without reference to further “stages” (or “times”). On the other hand, in topology the existence of cross-sections (over the whole space) for sheaves is rare compared to local existence, i.e. existence of sections over coverings. I.e., further “stages” must be taken into account.

5.6. DEFINITION. Let $\mathcal{C}$ be a site, F a sheaf and $a \in F(X)$. $X \models \exists x \varphi[a]$ iff there is a localization $(f_i: X_i \rightarrow X)_{i \in I}$ of X and a family $(b_i)_{i \in I}$ such that for every $i \in I$, $b_i \in F(X_i)$ and $X_i \models \varphi[b_i, F(f_i)(a)]$.

5.7. REMARK. A similar clause should be used to define $X \Vdash \varphi_1 \vee \varphi_2$. On the other hand, $\wedge$ is decided “on the spot” and $\Rightarrow, \forall$ are dealt with in the usual Kripke fashion, e.g.

$X \Vdash (\varphi \Rightarrow \psi)(a)$ iff for every $f: Y \rightarrow X$,

$Y \Vdash \varphi[F(f)(a)]$ implies $Y \Vdash \psi[F(f)(a)]$;

negation is $\Rightarrow \downarrow$, and $\downarrow$ is described by means of objects Y for which $\emptyset \in \text{Cov}(Y)$.

(ii) One can check that this notion of forcing specializes to the usual ones. As an example, assume e.g. $\mathcal{A} \Vdash^* (\varphi \vee \psi)[a]$ in the sense of ROBINSON [1971], i.e.,

$$\forall \mathcal{A} \xrightarrow{f} \mathcal{B} \in \text{Mod}(T) \exists \mathcal{B} \xrightarrow{g} \mathcal{L} \in \text{Mod}(T)$$

such that $\mathcal{L} \Vdash^* \varphi[gfa]$ or $\mathcal{L} \Vdash^* \psi[gfa]$. We may assume that $g = \Phi(f)$. Then the family

$$(\mathcal{A} \xrightarrow{\Phi(f) \circ f} \mathcal{L})_f$$

is a “co-localization” for $\neg \neg$. Furthermore, for every $\mathcal{L}$, $\mathcal{L} \Vdash^* \varphi[\Phi(f)fa]$ or $\mathcal{L} \Vdash^* \psi[\Phi(f)fa]$. We now use induction. (This example is taken from unpublished work by Joyal-Reyes.)

(iii) In the particular case that the site is a topos $\mathcal{E}$ (with the canonical localization) we have a way of interpreting languages (even infinitary ones). In particular we may define the notion of a T -model in $\mathcal{E}$, for any theory T (in a $L_{\infty\omega}$ -language, say), and the category of T -models in $\mathcal{E}$ as well. In case $\mathcal{E} = (\text{Sets})$, it amounts to this: its objects are set-theoretical models and its morphisms are “algebraic”, i.e. functions $f: \mathcal{A} \rightarrow \mathcal{B}$ which preserve the basic relations and operation symbols in the sense that $(a_1, \dots, a_n) \in R^{\mathcal{A}} \Rightarrow (f(a_1), \dots, f(a_n)) \in R^{\mathcal{B}}$ (with a corresponding clause for operation symbols).

For a semantics in terms of extensions, see 6.8.

5.8. PROPOSITION (Existence of a classifying topos; REYES [1974], in collaboration with Joyal). *For every finitary coherent theory T , there is a topos $\mathcal{E}[T]$ and a T -model M in $\mathcal{E}[T]$ which is generic in the sense that the category of T -models of $\mathcal{D}$ is equivalent (via M) to the category of geometric morphisms of $\mathcal{D}$ into $\mathcal{E}[T]$, for every topos $\mathcal{D}$.*

PROOF (outline). Let $\mathbf{R}$ be the logical category associated to T (Example

4.4). Then $\mathcal{E}[T]$ is the category of sheaves for $\mathbf{R}$ with the finite cover topology (Example 5.3(iii)). $\square$

5.9. REMARK. (i) The earliest example of the existence of classifying topos was given by HAKIM [1972], who proved that the Zariski topos is the classifying topos for the theory of local rings.

(ii) This theorem remains true for an arbitrary (i.e. infinitary) coherent theory. Furthermore, any topos is the classifying topos of such a theory (see MAKKAÏ and REYES [1976]).

6. Elementary topos

The word “elementary” in this context refers to the fact that the notion of elementary topos is an elementary notion: the notion of category with a few properties which are expressible in first order terms in the language of the theory of categories. It is even an “essentially algebraic” notion (FREYD [1972]).

The search for such a concept, as a foundation of mathematics, was initiated in LAWVERE [1964], but a more general notion comprising the notion of Grothendieck topos, and at the same time revealing the logical (even higher-order logical) nature of these, was found in 1969 by Lawvere and Tierney; see LAWVERE [1972]. With the simplifications now possible, KOCK and MIKKELSEN [1974], this very simple and powerful notion can be described as follows.

6.1. DEFINITION. An *elementary topos* $\mathcal{E}$ is a category with finite inverse limits and an object Ω which

- (i) classifies subobjects,
- (ii) is exponentiable.

6.2. REMARK. Here, (i) means that there is a universal subobject $true: 1 \rightarrow \Omega$, such that any subobject $A' \twoheadrightarrow A$ of any object A comes about as a pull-back

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & \Omega \\ \uparrow & & \uparrow \text{true} \\ A' & \longrightarrow & 1 \end{array}$$

for a unique α (“the characteristic function of A' ”); and (ii) means that for

each A , there is an object Ω^A ("the power object of A ") and a map $\in_A : A \times \Omega^A \rightarrow \Omega$, which establishes for each B a 1-1 correspondence

$$\frac{A \times B \xrightarrow{\beta} \Omega}{B \xrightarrow{\check{\beta}} \Omega^A} \quad (6.1)$$

in the following way: to $\check{\beta}$, associate

$$A \times B \xrightarrow{1 \times \check{\beta}} A \times \Omega^A \xrightarrow{\in_A} \Omega.$$

6.3. EXAMPLE. The model to have in mind is the category of sets, with Ω any two-element set, say the set consisting of the two symbols "true" and "false"; then Ω^A can be identified with the power set of A (since a subset $A' \subseteq A$ can be completely described by its characteristic function $\alpha : A \rightarrow \Omega$ given by

$$\begin{aligned} \alpha(a) &= \text{true} && \text{if } a \in A; \\ &= \text{false} && \text{if not.} \end{aligned}$$

What is important is first that each Grothendieck topos is also a model of these axioms, secondly that essentially all ("intuitionistically valid") higher order naive set theory follows from the simple axioms of Definition 6.1. From 1969 to now, a vast amount of papers etc. demonstrated how various notions and constructions of higher order naive set theory can be based on and carried out in the setting of an elementary topos. Instead of trying to survey all these, we give some detailed examples of constructions.

6.4. EXAMPLE. It is clear that Ω^A depends contravariantly on A , $f : A \rightarrow B$ gives rise to $\Omega^f : \Omega^B \rightarrow \Omega^A$ (which in (Sets) is the law which to a subset B' of B associates $f^{-1}(B') \subseteq A$). Also, Ω^A carries canonically the structure of an ordered object (in the set case: the inclusion ordering on the set of subsets of A). This structure is a subobject $\leq_A$,

$$\leq_A \twoheadrightarrow \Omega^A \times \Omega^A.$$

It has a characteristic function

$$\text{ch}(\leq_A) : \Omega^A \times \Omega^A \rightarrow \Omega$$

which, according to the exponential adjointness (6.1) corresponds to a map

$$\Omega^A \xrightarrow{\downarrow \text{seg}} \Omega^{\Omega^A}$$

which in the (Sets) case has the effect of associating to the subset $A \subseteq A$

the family of all subsets $A'' \subseteq A$ with $A'' \subseteq A'$ (the “down-segment of A' ”). The right adjoint $\forall_f$ of $\Omega^f : \Omega^B \rightarrow \Omega^A$ (for $f : A \rightarrow B$) can now be described as the composite

$$\Omega^A \xrightarrow{\downarrow \text{seg}} \Omega^{\Omega^A} \xrightarrow{\Omega^{\Omega^f}} \Omega^{\Omega^B} \xrightarrow{\Omega^{(\cdot)}} \Omega^B$$

where $\{\cdot\} : B \rightarrow \Omega^B$ corresponds under exponential adjointness to the characteristic map $B \times B \rightarrow \Omega$ of the diagonal $B \rightarrow B \times B$. In the (Sets)-case, the reader will see that the composite has the following effect on

$$A' \subseteq A$$

$$\begin{aligned} A' &\mapsto \{A'' \subseteq A \mid A'' \subseteq A'\} \mapsto \{B' \subseteq B \mid f^{-1}(B') \subseteq A'\} \\ &\mapsto \{b \in B \mid f^{-1}(\{b\}) \subseteq A'\} \\ &= \{b \in B \mid \forall a \in A : f(a) = b \Rightarrow a \in A'\} \end{aligned}$$

which we denote $\forall_f(A')$. Then it is easy set-theoretically to check that we do have a right adjoint for the inverse image formation, i.e. we have

$$f^{-1}(B') \subseteq A' \quad \text{iff} \quad B' \subseteq \forall_f(A').$$

Using this “internal universal quantification”, one can get an “intersection”-construction

$$\Omega^{\Omega^A} \xrightarrow{\cap} \Omega^A$$

which in (Sets) has the effect of associating to $\mathcal{F} \subseteq \Omega^A$ the set $\bigcap \mathcal{F} \subseteq A$ (the intersection of all $A' \in \mathcal{F}$). We omit that. Using this “intersection combinator”, one can derive the *left* adjoint $\exists_f$ (“direct image formation along f ”) as the composite

$$\Omega^A \xrightarrow{\uparrow \text{seg}} \Omega^{\Omega^A} \xrightarrow{\Omega^{\Omega^f}} \Omega^{\Omega^B} \xrightarrow{\cap} \Omega^B$$

($\uparrow \text{seg}$ defined dually of $\downarrow \text{seg}$). In (Sets) this map takes $A' \subseteq A$ into the intersection of all $B' \subseteq B$ with $f^{-1}(B') \supseteq A'$, which clearly is just $f(A')$. (The descriptions here are due to MIKKELSEN [1976]; it illustrates how one can derive colimit-type notions, like image-formation $\exists_f$, on basis of the axioms. For more about the basic theory, see KOCK and WRAITH [1971], KOCK and MIKKELSEN [1974], MACLANE [1975] or WRAITH [1975].)

We now describe how some more complicated notions of higher naive set theory get very simple formulations in the setting of elementary topoi. Observe that a binary relation on an object A

$$R \rightharpoonup A \times A$$

gives rise to a characteristic function $A \times A \rightarrow \Omega$, and then by the exponential adjointness to a map $r : A \rightarrow \Omega^A$ ("the down-segment for R "), and conversely, whence we also call a map $r : A \rightarrow \Omega^A$ a binary relation on A .

6.5. DEFINITION (OSIUS [1974]). A relation $r : A \rightarrow \Omega^A$ is said to be *recursive* (or (*strongly*) *well founded*) if for every B and $g : \Omega^B \rightarrow B$ there is a *unique* $f : A \rightarrow B$ making the diagram

$$\begin{array}{ccc} \Omega^A & \xrightarrow{\exists_f} & \Omega^B \\ r \downarrow & & \downarrow g \\ A & \xrightarrow{f} & B \end{array} \quad (6.2)$$

commute; and r is called (*weakly*) *well founded* if for each $g : \Omega^B \rightarrow B$, there is *at most* one f making (6.2) commute.

6.6. THEOREM (Mikkelsen; see OSIUS [1975a]). *The notions of strongly and weakly well founded relation agree in any elementary topos.*

PROOF. The quite difficult proof consists of course in constructing an f making (6.2) commute. Theorem 6.6 thus is the assertion that the principle of map-construction by transfinite recursion over (internally) well founded relations is valid inside any elementary topos. $\square$

6.7. REMARK. The fact that the recursion principle is valid in every topos may be interpreted proof-theoretically: it is intuitionistically provable. In fact, Fourman, COSTE [1974], BOILEAU [1975] (in collaboration with Joyal) have all set up formal systems of higher order intuitionistic type theory which are adequate and complete for elementary topoi. Thus elementary topoi may be viewed as a categorical version of intuitionistic higher order logic. Several results may be interpreted and proven in this context. This is discussed in detail in Chapter D.6.

As far as first-order intuitionistic logic in a topos is concerned, formal systems which again are adequate and complete for topoi have been set up by Benabou, Boileau, Coste, Dionne, Joyal, Makkai, Oullet, Reyes, Robitaille-Giguere (see COSTE [1973], OULET [1974], for Gentzen-type system, and ROBITAILLE-GIGUERE [1975] for a Hilbert-type system).

6.8. Semantics by extensions

The good exactness properties and the cartesian closedness which can be proved for any elementary topos can be used to prove that any first-order

formula (coherent or not) whose primitive relations have been interpreted by “extensions” have themselves “extensions”. The notion of *extension* of a formula can be defined as a universal element (in the sense of Kripke–Joyal semantics) satisfying the formula. (We think of $\mathcal{E}$ as a site by taking the finite cover topology.) A systematic description of this technique of forming extensions of formulas and proving inclusion relationships between such has been given by MITCHELL [1972], Benabou (COSTE [1973, 1974]) and OSIUS [1973]. The relationship to Kripke–Joyal semantics is analysed in OSIUS [1975b].

6.9. EXAMPLE. Let R be a ring object in an elementary topos, and form $GL(1, R) \subseteq R$ as the extension of the formula “ x is invertible” (or formally “ $\exists y: x \cdot y = 1$ ”). Also, for each natural number n , one may form the extension

$$[[\neg((x_1 = 0) \wedge \cdots \wedge (x_n = 0))]] \subseteq R^n \quad (6.3)$$

as well as the extension

$$[[(x_1 \text{ is invertible}) \vee \cdots \vee (x_n \text{ is invertible})]] \subseteq R^n. \quad (6.4)$$

6.10. DEFINITION. We say that R is a *field* object if for each n , the objects described in (6.3) and (6.4) agree (i.e. if R satisfies: “when n elements are not simultaneously zero, one of them is invertible, and conversely”). (This is a non-coherent notion.)

6.11. EXAMPLE (synthetic geometry, KOCK [1974]). Using the technique of extensions, and other exactness properties of an elementary topos $\mathcal{E}$ with a field object R , one can, following what one does in the (Sets) case, build some of the interesting objects of algebraic geometry, like Grassmannians. We shall illustrate this by constructing the projective $(n-1)$ -space $P^{n-1}(R)$. This is simply (6.3) (or (6.4)) modulo the equivalence relation induced on this object by the obvious action of $GL(1, R)$

$$P^{n-1}(R) = \left[\left[\bigvee_{i=1}^n x_i \text{ is invertible} \right] \right] / GL(1, R).$$

Also, one can carve out of the power object of $P^{n-1}(R)$ an object of $(n-2)$ -planes in $P^{n-1}(R)$, but it is more accessible to computation to construct this object by linear and multilinear algebra. In the case $P^2(R)$, for instance, one could define an object L (“of lines in $P^2(R)$ ”) purely algebraically. Also using 3×3 determinants, one can next form the extension of the notion “incidence”, i.e.,

$$[[\text{line } l \text{ passes through point } Q]] \subseteq L \times P^2(R).$$

One has now a model of a certain two-sorted first order structure with sorts “lines” and “points”, and one relation, “incidence”, and one may ask which sentences in this language hold for the structure thus constructed, in particular, does it satisfy the axioms of the notion of projective plane? It does, provided suitable of the non-equivalent intuitionistic forms of the axioms for “projective plane” are chosen. For details, see Kock [1974]. With suitable modifications, like saying “invertible” instead of “non-zero” wherever possible, the whole development can be carried through for a local ring object instead of a field object. The interest of this now is when it is carried out for the *generic* local ring object A in the classifying topos $\mathcal{X}$ for local rings (the Zariski topos).

It turns out (Kock [1974]) that this generic local ring is in fact a *field* object in the sense explained above, so that the construction of $P^2(A)$ and the other Grassmannians can be carried out using not only the technique of extensions, but also the assumption that A is a field. This $P^2(A)$, which as an object of $\mathcal{X}$ is a functor from finitely presented commutative rings to sets, agrees with the explicitly described such functor which in DEMAZURE and GABRIEL [1970] is honoured with this name. The theory of extensions allows us to get the geometric objects “by logical means” without having to produce functors and test sheaf-conditions; and it allows questions of *synthetic* geometry to be raised.

6.12. REMARK. Using the object $D \subseteq A$, the extension $[[x^2 = 0]]$, as “the infinitesimal object” as well as the fact that $\mathcal{X}$ is an elementary topos and thus has exponentiation, there seems to be a possibility of having even a synthetic differential geometry in $\mathcal{X}$ and related topos.

6.13. Arithmetic universe

A complete axiomatization of this notion (due to Joyal) seems not to exist, but the programme for what one wants to be axiomatized is the following: all structure of essentially algebraic nature (FREYD [1972]) which an elementary topos with natural number object has, and which is preserved by inverse image functors f^* . So an arithmetic universe is at least a pretopos with natural number object N (since f^* is a pretopos morphism which preserves N), but since an elementary topos with natural number object has, and f^* preserves, formation of free monoids, free categories on a graph of generators, formation of $\otimes$ product of abelian group objects, ..., all this may be included into the good axiomatics for arithmetic

universe in case it does not already follow from the existence of natural number object in a pretopos (which most of it does not). Joyal suggested: pretopos where free categories on graphs exist as an axiomatization. A *morphism* of arithmetic universe is a functor which preserves the pretopos structure and the added structure (free categories on graphs, say). If one includes formation of $\otimes$ of abelian groups into the structure, one can describe the notion of Hopf-algebra object (ring object A with a map $A \rightarrow A \otimes A$ satisfying certain equations) by functorial semantics by arithmetic universe. Classifying topos for the notion of Hopf algebra can be proved to exist.

7. Topoi and axiomatic set theory

Any model m of set theory (ZF, say) defines an elementary topos, $\mathcal{E}(m)$ the category of m -sets, whose objects are the elements ("sets") of m , and topoi arising this way are rather special (having the multitude of, say, Grothendieck topoi in mind). The question arises whether one can characterize topoi of form $\mathcal{E}(m)$ in elementary terms (a non-elementary characterization was given in LAWVERE [1964]).

This can also be viewed as the question of relative interpretation of a suitable extension of the first order theory of elementary topos into ZF, and vice versa.

The question of characterization (or mutual relative interpretation) was solved in 1971 by COLE [1971], MITCHELL [1972], and OSIUS [1974]. It is a matter of building models of set theory, out of a given elementary topos having suitable properties. Which properties are suitable?

First, the following propositions are evident.

7.1. PROPOSITION. *Any topos of form $\mathcal{E}(m)$ has the property that the terminal object 1 is a generator; and it is non-trivial: 0 not isomorphic to 1.*

That 1 is a generator means: if f, g are two different maps $X \rightrightarrows Y$ in $\mathcal{E}(m)$, then there is a map $x : 1 \rightarrow X$ such that $f \circ x \neq g \circ x$, and is clear since a map $x : 1 \rightarrow X$ corresponds to an element $x \in X$, viewing X as a "set" in m .

Clearly, the more properties of an elementary topos $\mathcal{E}$ one assumes, the stronger model of set theory one can build from it. The main idea of the construction is starting with an elementary topos with very few extra properties, and obtaining a model of a weak set theory. We give Osius'

form (OSIUS [1974]), which in view of 7.1 is “the minimal”. The set theory ZO resulting here lies between Zermelo–Thiele and Zermelo–Fraenkel (ZF), see OSIUS [1974].

7.2. THEOREM. *Given a non-trivial elementary topos $\mathcal{E}$ in which 1 is a generator. Then one can build a model of the set theory ZO.*

Before we give (a sketch of) the proof, we motivate and give the relevant definition. The main thing is a categorical characterization of transitive sets. If $A \in m$, then A is said to be *transitive* if $a \in A \Rightarrow a \subseteq A$. Denoting the (restriction of the) $\in$ -relation on A by R , and reinterpreting R as a map $r : A \rightarrow \Omega^A$ in $\mathcal{E}(m)$, we have that r is well-founded (in the sense explained in Section 6) and is a monic map, because $\in$ is well-founded and extensional in Zermelo–Thiele set theory.

We can even get the converse, and more (for m a ZF model).

7.3. THEOREM (Mostowski; see OSIUS [1974]). *In order that a relation $r : A \rightarrow \Omega^A$ on $A \in \mathcal{E}(m)$ is isomorphic to the $\in$ -relation on a transitive set, it is necessary and sufficient that r is well-founded (Definition 6.5) and monic as a map.*

7.4. THEOREM (OSIUS [1974]). *In order that a map $f : A_1 \rightarrow A_2$ between two transitive sets in m is the inclusion of $A_1 \subseteq A_2$, it is necessary and sufficient that*

$$\begin{array}{ccc} A_1 & \longrightarrow & A_2 \\ r_1 \downarrow & & \downarrow r_2 \\ \Omega^{A_1} & \xrightarrow{\exists_f} & \Omega^{A_2} \end{array} \quad (7.1)$$

commutes, where r_1 and r_2 are the $\in$ -relations on A_1 and A_2 .

So we have a structural characterization of transitive sets and of those maps between them which are inclusions.

7.5. PROOF OF THEOREM 7.2 (outline). We start by taking the conclusions of Theorems 7.3 and 7.4 as definitions. Let $\mathcal{E}$ be a non-trivial elementary topos where 1 is a generator.

7.6. DEFINITION. An object $A \in \mathcal{E}$ equipped with a relation $r : A \rightarrow \Omega^A$ is called a *transitive set object* (tr.s.o.) if r is monic and recursive (Definition

6.5). A map $f: A_1 \rightarrow A_2$ between two tr.s.o.'s (A_1, r_1) and (A_2, r_2) is called an *inclusion* if (7.1) commutes.

One now goes about proving that the category of tr.s.o.'s in $\mathcal{E}$, with inclusions as mappings, is equivalent (as a category) to a *lattice* (except that a maximal element is missing).

Now a model $m(\mathcal{E})$ for ZO can be constructed as follows: the elements in $m(\mathcal{E})$ are equivalence classes of pairs $((A, r), M)$, where (A, r) is a tr.s.o. and $M: A \rightarrow \Omega$ is a map (heuristically, thus M is (characteristic map of) a subset M' of a transitive set A). The equivalence relation is given by means of the lattice structure.

To describe the membership relation, one utilizes the family of maps

$$\{\Omega^A \times A \xrightarrow{\epsilon_A} \Omega \mid A \in |\mathcal{E}|\}$$

given by the topos structure of $\mathcal{E}$.

A more detailed comparison between mutual strengths of certain (stronger) systems of set theory, and some further strengthenings of the notion of elementary topos, is given in the works (OSIUS [1974], COLE [1971] and MITCHELL [1972]).

8. Other fields of research in categorical logic

We have not tried to be comprehensive. We would have liked also to include comments on:

8.1. Model completeness via sheaf categories (MACINTYRE [1973]).

8.2. Logical methods applied to sheaf categories on topological spaces and real number objects in elementary topoi (MULVEY [1974], SCOTT [1968], Stout, Tierney).

8.3. Topos theoretic interpretation of methods of non-standard analysis (KOCK and MIKKELSEN [1974], REYES [1974], TAKAHASHI [1975]).

8.4. Topos theoretic methods in independence proofs in set theory (TIERNEY [1972], BUNGE [1974]) — although this goes against the trend of letting the “topos” notion have the lead over the notion “model of set theory”.

8.5. Elementary topoi with a natural number object, and how an internal theory of classifying topos can be formed (Diaconescu, Tierney, Joyal, Johnstone, Lesaffre, De Kinder, WRAITH [1975], where references can be found).

8.6. Combinatorial logic and proof theory in form of cartesian closed categories (LAMBEK [1972], SZABO [1977] and SCOTT [1972]).

References

ANTONIUS, W.

[1975] Théories cohérentes et prétopos, Thèse, Université de Montréal, Montreal.

BARR, M.

[1974] Toposes without points, *J. Pure Appl. Algebra*, **5**, 265–280.

BASTIANI, A. and C. EHRESMANN

[1972] Categories of sketched structures, *Cahiers Topologie Géom. Différentielle*, **13**, 105–214.

BENABOU, J.

[1973] Catégories et logiques faibles, Tagungsbericht, Oberwolfach.

BOILEAU, A.

[1974] Les multiples splendeurs de forcing, Thèse de Maîtrise, Université de Montréal, Montreal.

[1975] Types versus topos, Université de Montréal, Montreal, mimeographed.

BUNGE, M.

[1974] Topos theory and Souslin's hypothesis, *J. Pure Appl. Algebra*, **4**, 159–188.

COHN, P.M.

[1965] *Universal algebra* (Harper & Row, New York).

COLE, J.

[1971] Categories of sets and models of set theory, in: *Proceedings of the Bertrand Russell Memorial Logic Conference*, Uldum, Denmark.

COSTE, M.

[1973] Logique du 1^{er} ordre dans les topos élémentaires, Séminaire Benabou, Paris.

[1974] Logique d'ordre supérieur dans les topos élémentaires, Séminaire Benabou, Paris.

DEMAZURE, M. and P. GABRIEL

[1970] *Groupes Algébriques*, I (North-Holland, Amsterdam).

DIONNE, J.

[1973] Des théories élémentaires aux catégories conceptuelles, et Addendum, Thèse, Université de Montréal, Montreal.

FREYD, P.

[1966] Algebra-valued functors in general and tensor products in particular, *Colloq. Math.*, **14**, 89–106.

[1972] Aspects of topoi, *Bull. Austral. Math. Soc.*, **7**, 1–76.

[1973] Allegories, Université de Montréal, Montreal, preprint.

GROTHENDIECK, A., et al., editors

[1963–] *Théorie des Topos et Cohomologie Étales des Schémas*, Tome 1 and 2, Lecture

[1972] Notes in Mathematics, Vols. 269–270 (Springer, Berlin).

GABRIEL, P. and F. ULMER

[1971] *Lokal Präsentierbare Kategorien*, Lecture Notes in Mathematics, Vol. 221 (Springer, Berlin)

HAKIM, M.

[1972] *Topos Annelés et Schemas Relatifs*, Ergebnisse, Vol. 64 (Springer, Berlin).

HIGGS, D.

[1976] A category approach to boolean valued set theory, to appear.

JOYAL, A.

[1971] Polyadic spaces and elementary theories, *Notices Am. Math. Soc.*, **18** (3), 967.

[1975] Les théorèmes de Chevalley–Tarski et remarque sur l'algèbre constructive, *Cahiers Topologie Géom. Différentielle*, **16**, 256–258.

KEANE, O.

[1975] Abstract Horn theories, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin) pp. 15–50.

KOCK, A.

- [1974] Linear algebra and projective geometry in the Zariski topos. Aarhus Preprint Series, No. 4 (revised version in *J. Pure Appl. Algebra*, to appear).

KOCK, A. and C.J. MIKKELSEN

- [1974] Topos theoretic factorization of non-standard extensions, in: *Victoria Symposium on Nonstandard Analysis* 1972, Lecture Notes in Mathematics, Vol. 369 (Springer, Berlin) pp. 122-143.

KOCK, A. and G.C. WRAITH

- [1971] *Elementary Toposes*, Aarhus Lecture Notes Series, No. 30.

LAWVERE, F.W.

- [1963] Functorial semantics of algebraic theories, *Proc. Nat. Acad. Sci. U.S.A.*, **50**, 869-872.
- [1964] An elementary theory of the category of sets, *Proc. Nat. Acad. Sci. U.S.A.*, **52**, 329-334.
- [1965a] Algebraic theories, algebraic categories, and algebraic functors, in: *The Theory of Models* (North-Holland, Amsterdam) pp. 413-418.
- [1965b] Functorial semantics of elementary theories, in: *Logic Colloquium*, Leicester.
- [1969] Adjointness in foundations, *Dialectica*, **23**, 281-296.
- [1970] Equality in hyperdoctrines and comprehension schema as an adjoint functor, *Proc. Am. Math. Soc.*, 1-14.
- [1972] Introduction, in: *Toposes, Algebraic Geometry and Logic* (Halifax 1971), edited by F.W. Lawvere, Lecture Notes in Mathematics, Vol. 274 (Springer, Berlin).
- [1975a] Introduction to Part I, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin) pp. 3-14.
- [1975b] Continuously variable sets; algebraic geometry = geometric logic, in: *Logic Colloquium '73*, edited by H.E. Rose and J.C. Shepherdson (North-Holland, Amsterdam) pp. 135-156.

LAZARD, M.

- [1955] Lois de groupes et analyseurs, *Ann. Écoles Norm. Sup.*, **72** (3), 299-400

MACLANE, S.

- [1975] Sets, topoi and internal logic in categories, in: *Logic Colloquium '73*, edited by H.E. Rose and J.C. Shepherdson (North-Holland, Amsterdam) pp. 119-134.

MACINTYRE, A.

- [1973] Model completeness for sheaves of structures, *Fund. Math.*, **81**, 73-89.

MAKKAI, M. and G.E. REYES

- [1976] Model theoretic methods in the theory of topoi and related categories, I, II, *Bull. Acad. Polon. Sci.*, **24**, 379-392.

MIKKELSEN, C.J.

- [1976] Lattice theoretic and logical aspects of elementary topoi, Thesis, Aarhus Various Publications Series No. 25.

MITCHELL, W.

- [1972] Boolean topoi and the theory of sets, *J. Pure Appl. Algebra*, **2**, 261-274.

MULVEY, C.

- [1974] Intuitionistic algebra and representations of rings, *Mem. Am. Math. Soc.*, **148**, 3-57.

OSIUS, G.

- [1973] The internal and external aspect of logic and set theory in elementary topoi, *Cahiers Topologie Geom. Differentielle*, **14**, 47-49.
- [1974] Categorical set theory: A characterization of the category of sets, *J. Pure Appl. Algebra*, **4**, 79-119.

- [1975a] Logical and set theoretical tools in elementary topoi, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin) pp. 297–346.
- [1975b] A note on Kripke–Joyal semantics for the internal language of topoi, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin) pp. 349–354.
- OULLET, R.
 - [1974] Axiomatisation de la logique interne du premier ordre des topos, version inclusive et multisorte, These, Université de Montréal, Montreal.
- REYES, G.
 - [1974] From sheaves to logic, in: *M.A.A. Studies in Mathematics*, Vol. 9, edited by A. Daigneault (Math. Assoc. Am., NY) pp. 143–204.
- ROBINSON, A.
 - [1971] Infinite forcing in model theory, *Proceedings of the 2nd Scandinavian Logic Symposium*, edited by J.E. Fenstad (North-Holland, Amsterdam) pp. 317–340.
- ROBITAILLE-GIGUERE, M.
 - [1975] Modèles d'une categorie logique dans de topos de prefaisceaux et d'ensembles de Heyting, Thèse, Université de Montréal, Montreal.
- SCHUBERT, H.
 - [1970] *Kategorien II*, Heidelberger Taschenbücher (Springer, Berlin).
- SCOTT, D.
 - [1968] Extending the topological interpretation to intuitionistic analysis, in: *Logic and Foundations of Mathematics* (Wolters-Noordhoff, Groningen).
 - [1972] Continuous lattices, in: *Toposes, Algebraic Geometry and Logic* (Halifax 1971), edited by F.W. Lawvere, Lecture Notes in Mathematics, Vol. 274 (Springer, Berlin) pp. 97–136.
- SZABO, M.E.
 - [1977] *Algebra of Proofs* (North-Holland, Amsterdam).
- TAKAHASHI, S.
 - [1975] *Géometrie Diophantienne* (Presses de l'Université de Montréal, Montreal).
- TIERNEY, M.
 - [1972] Sheaf theory and the continuum hypothesis, in: *Toposes. Algebraic Geometry and Logic* (Halifax 1971), edited by F.W. Lawvere, Lecture Notes in Mathematics, Vol. 274 (Springer, Berlin).
- VOLGER, H.
 - [1975] Completeness theorem for logical categories, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin).
- WRAITH, G.C.
 - [1969] *Algebraic Theories*, Aarhus Lecture Notes Series, No. 22, revised version, 1975.
 - [1975] Lectures on elementary topoi, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin) pp. 51–86.

PART B

Set Theory

Guide to Part B: *Set Theory*

with the cooperation of
K. KUNEN

B.1. SHOENFIELD	
<i>The axioms of set theory</i>	321
B.2. JECH	
<i>About the axiom of choice</i>	345
B.3. KUNEN	
<i>Combinatorics</i>	371
B.4. BURGESS	
<i>Forcing</i>	403
B.5. DEVLIN	
<i>Constructibility</i>	453
B.6. RUDIN	
<i>Martin's Axiom</i>	491
B.7. JUHÁSZ	
<i>Consistency results in topology</i>	503

The advances in set theory which followed the initial discoveries of Gödel and Cohen have sent shockwaves of independence results throughout several parts of mathematics. The main thrust of this part of the Handbook is toward explaining to the mathematician many of the important methods and results which have emerged.

The introductory chapter is by J. Shoenfield. In it he describes the intuitive universe of all sets and the axiomatic set theory ZF to which it gives rise. This chapter is strongly recommended for anyone who doesn't know what ZF is, or who does know but has the impression that the axioms arise in an ad hoc attempt to eliminate the paradoxes.

Jech's chapter, which follows, explains the special status of AC — the axiom of choice. It discusses the uses of the axiom of choice in mathematics

and how mathematics would look without AC. It also contains an introduction to the consistency and independence results surrounding AC.

A first-order sentence φ is *consistent* with ZF if one cannot prove $\neg\varphi$, the negation of φ , from the axioms of ZF. To put it another way, φ is consistent with ZF if the theory $\text{ZF} + \varphi$ does not give rise to any contradictions. The sentence φ is *independent* of ZF if φ is not a theorem of ZF, that is, if $\neg\varphi$ is consistent with ZF. There are two ways to establish the consistency of a mathematical statement with set theory — the easy way and the hard way.

The easy way to prove some sentence φ consistent with ZF is to find some other sentence ψ which is already known to be consistent with ZF and then prove (in ZF) that ψ implies φ . There are several good candidates for ψ which have emerged. The mathematician who is familiar with these need know no logic whatsoever in order to prove consistency results. We mention, in particular, Martin's axiom MA, the continuum hypothesis CH and the stronger principle $\diamond$ of Jensen. Martin's axiom and its uses are discussed in M.E. Rudin's chapter. Uses of CH and $\diamond$ are discussed in the chapters of Kunen and Juhász.

The hard way to prove a consistency result is to go back to basics and build a model. Thus, if we want to show that φ is consistent with ZF we construct a model $\mathcal{M}$ of the axioms of ZF (and hence of the theorems of ZF) in which φ is true.

The first such construction of a model of ZF was Gödel's universe L of constructible sets. This is a very natural model — it is the smallest model of ZF containing all the ordinals. Gödel showed that both AC and the continuum hypothesis CH are true in the model L , and hence are consistent with set theory. Jensen has studied L in depth and has discovered many beautiful properties of this model, like the principle $\diamond$ mentioned above. This work of Gödel and Jensen is surveyed in Devlin's chapter.

After L , the best way to construct models of ZF is Cohen's method of forcing. Cohen invented the method to prove the independence of AC and CH. Solovay and others have refined and simplified forcing so that by now it is a very powerful and not too complicated method for obtaining consistency results. Burgess, in his chapter, explains forcing in a way that should allow the non-logician to construct his own independence proofs. The early parts of this chapter, on absoluteness, are needed in Devlin's chapter.

Kunen's chapter is of a rather different nature in that it requires no knowledge of mathematical logic. It discusses infinitary combinatorial

principles of set theory, some of which have come from logic, which have far-reaching applications. In particular, he shows how to view AC, CH and $\diamond$ as progressively stronger “enumeration” principles, and when each should be used. He also discusses Ramsey’s theorem and uncountable generalizations of it which have proven important, ending with a discussion of large cardinal properties of a combinatorial nature. Other large cardinal properties are discussed, with suggested reading, in an appendix.

Among the chapters in other parts of the Handbook which are relevant to set theory are Martin’s chapter on descriptive set theory (in Part C) and the last section of Morley’s chapter (in Part A) on homogenous sets, where applications of large cardinals to L are discussed. Section 4 of Simpson’s chapter (in Part C) discusses some uses of extra set-theoretic hypotheses in the study of degrees of unsolvability.

B.1

Axioms of Set Theory

J.R. SHOENFIELD

Contents

1. Introduction	322
2. Sets and set formation	322
3. The axioms	324
4. Development of set theory	327
5. Ordinals	330
6. The Axiom of Choice	335
7. Classes	338
8. New axioms	341

1. Introduction

Ideally, an axiom system is formed as follows. First, we select the basic concepts and explain their nature as fully as possible. Then we write down axioms for the concepts. If all goes well, our explanation will make it clear that the axioms are true.

We will try to present the axioms of set theory in this fashion. We will therefore begin with an explanation of the notion of a set. Our explanation may appear surprisingly complicated to the mathematician who feels that he understands sets perfectly well. However, we shall see that this explanation is quite useful, not only for justifying the axioms of set theory, but also for investigating new axioms and for proving theorems about sets.

The ideas presented here have been developed gradually during the past century. Although they are well known to most set-theorists, they have rarely appeared in print in a coherent form. This explains the lack of a bibliography.

2. Sets and set formation

How shall we explain the notion of a set? As a first approximation, a set is a collection of objects. Thus a set is formed by selecting certain objects, called the *members* of the set; and the set is completely determined by its members.

The objects which are members of sets may be of any kind. In particular, we want to consider a set as an object and thus to allow it to be a member of another set. All objects other than sets which are used as members of sets are called *urelements*.

Even without using urelements, we can form many sets. We can form the empty set $\emptyset$; the set $\{\emptyset\}$ whose only member is $\emptyset$; the set whose only members are $\emptyset$ and $\{\emptyset\}$; and so on. We shall confine our attention to such sets, and shall use x , y , and z to represent such sets only. We shall explain later why nothing is lost by this.

We have now reached the following point: a set x is formed by choosing the sets which are to be members of x . Are there any restrictions on the sets which we may pick? There are, as the paradoxes of set theory show.

Let us recall the Russell paradox. Let r be the set whose members are all sets x such that x is not a member of x . Then for every set x ,

$$x \in r \leftrightarrow x \notin x. \quad (1)$$

Substituting r for x , we get a contradiction.

The explanation is not really difficult. When we are forming a set z by choosing its members, we do not yet have the object z , and hence cannot use it as a member of z . The same reasoning shows that certain other sets cannot be members of z . For example, suppose that $z \in y$. Then we cannot form y until we have formed z . Hence y is not available as an object when z is formed, and therefore cannot be a member of z .

Putting the matter in a positive way, a set z can have as members only those sets which are formed before¹ z . Thus for the set r formed above, (1) holds only for sets x formed before r ; so we cannot substitute r for x .

Carrying the analysis a bit further, we arrive at the following. Sets are formed in *stages*. For each stage S , there are certain stages which are *before* S . At stage S , each collection consisting of sets formed at stages before S is formed into a set.² There are no sets other than the sets which are formed at the stages.

This gives a reasonably clear explanation of the notion of a *set* in terms of the notions of a *stage* and of *before*. What can we say about these notions? We should certainly expect *before* to be a partial ordering of the stages; and this is the only fact about this relation which we need for our axioms.

Stages are important to us because they enable us to form sets. Thus suppose that x is a collection of sets and that S is a collection of stages such that each member of x is formed at a stage which is a member of S . If there is a stage after all of the members of S , then we can form x at this stage. Thus the fundamental question for us is: given a collection S of stages, is there a stage after all of the members of S ?

We would like the answer to this question to be yes whenever possible. We know by the paradoxes that not every collection of sets is a set; but we have avoided the paradoxes by restricting ourselves to sets which are formed at some stage. We do not wish to further restrict the notion of a set by not having sufficiently many stages.

Nevertheless, the answer to our question cannot always be yes. For example, if S is the collection of all stages, then there is no stage after every stage in S .

A possible answer to our fundamental question is this: there is a stage after all the stages in S provided that we can imagine a situation in which

¹ We should interpret *before* here in a logical rather than a temporal sense. It is similar to what we mean when we say that one theorem must be proved before another.

² Note that this means that if a set is formed at stage S , it can also be formed at every later stage. We could arrange things so that each set is formed at exactly one stage; but there is no point in doing so

all of the stages in S have been completed. In the case in which S contains all stages, we cannot imagine such a situation, since we can always imagine a further stage. At best, this is a very vague answer; for it is not at all clear in general what we can or cannot imagine. It does, however, provide a useful guide for obtaining more precise principles on which we can base axioms.

Specifically, there are three cases in which our vague answer leads us to conclude that there is a stage after each member of S . The first is the case in which S consists of a single stage. The second is that in which S consists of an infinite sequence $S_0, S_1, \dots$ of stages. The third case is that in which we have a set x and a stage S_y for each y in x , and S consists of the stages S_y for y in x .

In the first two cases, it is clear that we can imagine a situation in which all of the stages in S have been completed. In the third case, we can argue as follows. Suppose that as each stage S is completed, we take each y in x which is formed at S and complete the stage S_y . When we reach the stage at which x is formed, we will have formed each y in x and hence completed each stage S_y in S .

We have now progressed sufficiently far in our analysis to obtain the usual axioms of set theory. There are still many obscure points at which further analysis might lead to a better understanding of the axioms or to new axioms. We shall call attention to some of these as we proceed.

It is, of course, possible that there is a completely different analysis of the notion of a set, and this might lead to quite a different set of axioms. Up to the present, however, there has been no analysis of the notion of a set essentially different from that given here which leads to a satisfactory system of axioms.

3. The axioms

Before turning to the axioms, we must describe the language of set theory. This language has *set variables* $x, y, z, \dots$ which represent arbitrary sets. It also has the symbol $\in$ for the membership relation.

The rest of the notation is logical. We have the symbol $=$ for *is identical with*. We have the propositional connectives: $\neg$ for *not*, $\vee$ for *or*, $\wedge$ for *and*, $\rightarrow$ for *implies*, and $\leftrightarrow$ for *iff*. We have the quantifiers: $\forall$ for *for all*, $\exists$ for *for some*, and $\exists!$ for *for exactly one*. The variables following a quantifier may be restricted to belong to some set; e.g., $\forall x \in y$ means *for all x in y* .

Of course some of this logical notation could be defined in terms of the rest; but we are interested in set theory, not logic. For this reason, we shall

not bother to state the axioms of first-order logic, nor even the precise definition of a formula of first-order logic. These are discussed at length in the introductory chapter of Barwise (Chapter A.1).

We will recall from logic how operations are introduced. A unary operation F is introduced by defining $F(x)$ to be the unique y such that $\varphi(x, y)$ (where $\varphi(x, y)$ is some formula of the language not containing F). More precisely, we first prove $\forall x \exists! y \varphi(x, y)$, and then introduce F by the axiom $\varphi(x, F(x))$. A formula $\psi(F(x))$ containing F can then be interpreted as an abbreviation of $\exists y (\varphi(x, y) \wedge \psi(y))$. Binary and n -ary operations are treated similarly.

Remark: We allow an operation to depend upon parameters. Thus we might set $F(x) = x \cup y$, so that F depends upon y .

Now we can turn to the axioms. The first point in our analysis was that a set is entirely determined by its members. This is the content of our first axiom.

EXTENSIONALITY AXIOM: $\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y$.

One of the most important points established by our analysis is that certain collections of sets are sets. In translating this into our language, we face a difficulty: there is no general method of talking about collections in this language before we know that they are sets. There are, however, certain collections which we can talk about. Given a formula $\varphi(x)$, we can say certain things about the collection of all sets x such that $\varphi(x)$. In particular, we can say that it is a set as follows: $\exists y \forall x (x \in y \leftrightarrow \varphi(x))$. We abbreviate this expression to $\text{Set}\{x: \varphi(x)\}$.

Our first principle of set existence is: if every member of a collection of sets belongs to the set x , then that collection is a set. To see this, suppose that x is formed at stage S . Then every member of x is formed before S , and hence so is every member of the collection. Hence the collection can be formed into a set at stage S . We express this principle in our next axiom.

SEPARATION AXIOM: $\forall x (\varphi(x) \rightarrow x \in y) \rightarrow \text{Set}\{x: \varphi(x)\}$.

Note that the Separation Axiom is not a single axiom, but an infinite set of axioms, one for each formula $\varphi(x)$. (The name comes from the fact that we are separating those x which satisfy $\varphi(x)$ from those which do not.)

Our next principle is: the union of all the members of a set x is a set. For suppose that x is formed at S . Then every member of x is formed before S , and hence every member of a member of x is formed before S . This means that every member of the union is formed before S ; so the union can be formed at S . Our next axiom states this principle.

UNION AXIOM: $\text{Set}\{z: \exists y \in x (z \in y)\}$.

The next principle is: if x is any set, the collection of all subsets of x is a set. For suppose x is formed at S . Since every member of x is formed before S , every subset of x is formed at S . Thus the set of all subsets of x can be formed at any stage after S .

To state this principle as an axiom, we define:

$$x \subseteq y \leftrightarrow \forall z (z \in x \rightarrow z \in y).$$

POWER SET AXIOM: $\text{Set}\{y: y \subseteq x\}$.

Our next principle is: if F is a unary operation and x is a set, then the collection of all $F(y)$ for $y \in x$ is a set. To see this, let S_y be a stage at which $F(y)$ is formed. Then there is a stage S after all the stages S_y for $y \in x$. At stage S , we can form the desired set.

REPLACEMENT AXIOM: $\text{Set}\{z: \exists y \in x (z = F(y))\}$.

Our next axiom guarantees the existence of an infinite set. It is a bit complicated because we have no direct way in our language to say that a set is infinite.

INFINITY AXIOM: $\exists x (\exists y \in x \forall z (z \notin y))$

$$\wedge \forall y \in x \exists z \in x \forall w (w \in z \leftrightarrow w \in y \vee w = y)).$$

Let us see why the Infinity Axiom is true. Let x_0 be the empty set, and for each n , let x_{n+1} be the set whose members are the members of x_n and x_n itself. We can form x_0 at any stage; and if x_n is formed at some stage, then x_{n+1} can be formed at any later stage. Suppose that x_n is formed at S_n . Then there is a stage S after all of the S_n . At this stage, we can form the set x whose members are $x_0, x_1, \dots$. This x is the set which the Infinity Axiom says exists.

A member y of x is a *minimal member* of x if y and x have no member in common. Our next axiom states that every non-empty set has a minimal member.

REGULARITY AXIOM: $\exists y (y \in x) \rightarrow \exists y \in x \forall z \in y (z \notin x)$.

We will now show why the Regularity Axiom is true. We say that a stage S is *minimal* for x if some member of x is formed at S but no member of x is formed before S . If S is minimal for x and y is a member of x formed at S , then y is a minimal member of x ; for every member of y is formed before S and therefore cannot be in x .

It will thus suffice to show that for every non-empty set x , there is a stage

which is minimal for x . This has often been taken as an evident property of stages. However, we shall give a proof (due to Dana Scott) that this follows from the facts we already know about stages.

A set x is *grounded* if every set containing x has a minimal member. (Of course, when we know that the Regularity Axiom is true, we will know that every set is grounded.)

If every member of x is grounded, then x is grounded. For let $x \in y$. If x and y are disjoint, then x is the required minimal member of y . If not, then y contains a member of x , which is grounded by hypothesis. Hence again y has a minimal member.

For each stage S , let G_S be the set of all grounded sets formed before S . This is certainly a set, since it can be formed at S ; and it is grounded by the previous paragraph. If T is before S , then G_T is grounded and is formed at T which is before S ; so $G_T \in G_S$.

Now let x be a non-empty set. Say x is formed at S . Let y be the set of all G_T , where T is before S and some member of x is formed at T . This is a set, since each such G_T is formed before S . It is non-empty (because x is non-empty) and all of its members are grounded. Hence y has a minimal member G_T . We claim that T is minimal for x . If not, there is a stage U before T at which a member of x is constructed. By the above, $G_U \in G_T$; and, since U is before S , $G_U \in y$. This contradicts the choice of G_T . Our proof is complete.

We shall later add one more axiom, the Axiom of Choice. The axiom system consisting of these axioms is designated by ZFC. It is generally considered as the standard set of axioms for set theory.

4. Development of set theory

We are not going to give a detailed development of set theory, but are merely going to indicate how the various axioms are used in the development.

We will use $\{x: \varphi(x)\}$ for the set of x such that $\varphi(x)$. More formally, $\{x: \varphi(x)\}$ is introduced by the axiom

$$\forall x (x \in \{x: \varphi(x)\} \leftrightarrow \varphi(x)).$$

Thus before using this expression, we must prove

$$\exists! y \forall x (x \in y \leftrightarrow \varphi(x)).$$

Now if there is such a y , it is unique by the Extensionality Axiom; and the

statement that such a y exists is just $\text{Set}\{x: \varphi(x)\}$. Thus we may use $\{x: \varphi(x)\}$ only when we have proved $\text{Set}\{x: \varphi(x)\}$.

We shall write $\{F(x): \varphi(x)\}$ for $\{y: \exists x (\varphi(x) \wedge y = F(x))\}$. Thus the Replacement Axiom is $\text{Set}\{F(x): x \in y\}$.

The first task is to define the usual operations of set theory. The main function of the axioms here is to show that the sets needed exist. We sketch how this is done.

First we define the empty set:

$$\emptyset = \{x: x \neq x\}.$$

To show that this exists, let y be any set. (The Infinity Axiom shows that there is a set. Alternatively, one can use the usual axioms of logic to conclude that there is at least one set.) Then $\forall x (x \neq x \rightarrow x \in y)$; so $\text{Set}\{x: x \neq x\}$ by the Separation Axiom.

Next we define

$$\text{Un}(z) = \{x: \exists y \in z (x \in y)\},$$

$$\mathcal{P}(y) = \{x: x \subseteq y\}.$$

These sets exist by the Union Axiom and the Power Set Axiom. We call $\text{Un}(z)$ the *union* of z and $\mathcal{P}(y)$ the *power set* of y .

Now we define the set consisting of x and y :

$$\{x, y\} = \{z: z = x \vee z = y\}.$$

It is a little work to see that this set exists. Define an operation F by $F(\emptyset) = x$, $F(w) = y$ if $w \neq \emptyset$. If v is any set, $\{F(w): w \in v\}$ is a set by the Replacement Axiom. Hence by the Separation Axiom, it suffices to choose v so that x and y are in $\{F(w): w \in v\}$. This means that v must contain $\emptyset$ and a set other than $\emptyset$. It is easy to see that $v = \mathcal{P}(\mathcal{P}(\emptyset))$ will do.

Now we can define the Boolean operations:

$$x \cup y = \text{Un}(\{x, y\}),$$

$$x \cap y = \{z: z \in x \wedge z \in y\},$$

$$x - y = \{z: z \in x \wedge z \notin y\}.$$

The last two sets exist by the Separation Axiom.

Now we can define the set whose members are $x_1, \dots, x_n$ by induction on n :

$$\{x_1\} = \{x_1, x_1\},$$

$$\{x_1, \dots, x_{n+1}\} = \{x_1, \dots, x_n\} \cup \{x_{n+1}\}.$$

Other set operations are now easily defined.

Set theory deals not only with sets, but also with relations and functions, which are sets of ordered pairs.³ The ordered pair $\langle x, y \rangle$ is generally not thought of as a set; but we can identify it with a set if this set does everything we want the ordered pair to do. But all we want the ordered pair to do is specify its first and second element. In other words, the only essential property of the ordered pair is

$$\langle x, y \rangle = \langle z, w \rangle \rightarrow x = z \wedge y = w. \quad (2)$$

There are several definitions of $\langle x, y \rangle$ which will achieve this; the simplest is

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}.$$

We leave it to the reader to verify (2).

We can now define the Cartesian product:

$$x \times y = \{\langle z, w \rangle : z \in x \wedge w \in y\}.$$

To show that this exists, note that

$$z \in x \wedge w \in y \rightarrow \langle z, w \rangle \in \mathcal{P}(\mathcal{P}(x \cup y))$$

and then use the Separation Axiom.

One application is the extension of the Replacement Axiom to two (or more) arguments:

$$\text{Set}\{F(z, w) : z \in x \wedge w \in y\}. \quad (3)$$

For this, define a new operation G by $G(\langle z, w \rangle) = F(z, w)$ and $G(v) = 0$ if v is not an ordered pair. (This is a legitimate definition by (2).) Then

$$\{F(z, w) : z \in x \wedge w \in y\} = \{G(v) : v \in x \times y\};$$

so (3) follows from the Replacement Axiom.

Now we are going to show that our theory can also deal with the usual objects of mathematics. These are usually formed by set-theoretic operations from numbers. Now it is well known that all numbers (real, complex, integral and rational) can be constructed from the natural numbers (again using set-theoretical operations). We will show how to define the natural numbers in ZFC.

It is obvious that each natural number n must be identified with a set; which set shall we choose? It is natural to choose a set having n members; and the obvious such set is the set of natural numbers less than n . Thus the number 0 is identified with the empty set, 1 is identified with $\{0\}$, 2 with

³ We identify a function f with the set of all ordered pairs of the form $\langle f(x), x \rangle$, rather than the set of all ordered pairs $\langle x, f(x) \rangle$.

$\{0, 1\}$, and so on. This makes it clear that the successor operation must be defined by

$$Sc(x) = x \cup \{x\}.$$

Now say that a set is *inductive* if it contains $\emptyset$ and is closed under the successor operation. We then define a *natural number* to be a set which belongs to every inductive set.

It remains to prove the Peano axioms. The only one which gives any problem is

$$Sc(x) = Sc(y) \rightarrow x = y. \quad (4)$$

Suppose that $Sc(x) = Sc(y)$. By the Regularity Axiom, $\{x, y\}$ has a minimal element; and by symmetry, we may suppose that this is y . Then $x \notin y$. Now $x \in Sc(x) = Sc(y) = y \cup \{y\}$; so $x \in y$ or $x = y$. Hence $x = y$. (For the case in which x and y are natural numbers, (4) can be proved without using the Axiom of Regularity. However, (4) is sometimes useful for arbitrary sets x and y .)

The Infinity Axiom says that an inductive set exist. From this and the Separation Axiom, we see that the set of natural numbers exists.

We can now see why urelements are unnecessary: all of the objects we wish to consider are sets, or at least can be identified with sets. Actually, it would require only a little additional effort to reformulate our axiom system to allow urelements, and this would be useful for some purposes.

It is rather suprising that we can define all of the usual objects of mathematics and prove their properties in ZFC. Certainly this shows that ZFC is a very strong axiom system. We should not, however, make too much of this fact. To identify mathematics with ZFC (or to say, somewhat mysteriously, that ZFC is a foundation for mathematics) is both useless and misleading. It leads one to think that objects which are not definable in ZFC are not mathematical objects, and that truths which cannot be proved in ZFC are not mathematical truths. This is an unfruitful limitation on mathematics.

5 Ordinals

Although stages entered into our description of sets, they did not enter into the axioms. We shall show that nothing is lost thereby; we can define the stages and prove that they have the appropriate properties in ZFC.

We intend to identify the stages with certain sets, which we call *ordinals*. Roughly speaking, the ordinals are obtained by extending the sequence of natural numbers.

A set x is *transitive* if every member of x is a subset of x . An *ordinal* is a transitive set x such that every member of x is transitive. We use Greek letters for ordinals

5.1. THEOREM. *The set 0 is an ordinal. If α is an ordinal, then $\text{Sc}(\alpha)$ is an ordinal.*

PROOF. The easy proof is left to the reader. $\square$

COROLLARY. *Every natural number is an ordinal.*

5.2. THEOREM. *Every member of an ordinal is an ordinal.*

PROOF. Let $x \in \alpha$. Then x is transitive; so we need only show that every member y of x is transitive. Since α is transitive, $x \subseteq \alpha$; so $y \in \alpha$, and hence y is transitive. $\square$

We define

$$\alpha < \beta \leftrightarrow \alpha \in \beta,$$

$$\alpha \leq \beta \leftrightarrow \alpha < \beta \vee \alpha = \beta.$$

We first show that $<$ partially orders the ordinals, i.e., that

$$\neg(\alpha < \alpha), \tag{5}$$

$$\alpha < \beta \wedge \beta < \gamma \rightarrow \alpha < \gamma. \tag{6}$$

By the Regularity Axiom, α is a minimal member of $\{\alpha\}$. This means that $\alpha \notin \alpha$, which is (5). As for (6), it is a consequence of the transitivity of γ . $\square$

5.3. THEOREM. *If $\forall \alpha (\forall \beta < \alpha \varphi(\beta) \rightarrow \varphi(\alpha))$, then $\forall \alpha \varphi(\alpha)$.*

PROOF. We assume that the hypothesis holds and that $\neg \varphi(\alpha_0)$, and derive a contradiction. Let

$$x = \{\alpha : \alpha < \alpha_0 \wedge \neg \varphi(\alpha)\};$$

this set exists because each such α is in α_0 . Moreover, $x \neq 0$; for otherwise the hypothesis would give $\varphi(\alpha_0)$. Thus x has a minimal member α . If $\beta < \alpha$, then $\beta < \alpha_0$ by (6) and $\beta \notin x$ by choice of α . Thus $\varphi(\beta)$. The hypothesis now gives $\varphi(\alpha)$, contradicting $\alpha \in x$. $\square$

Theorem 5.3 tells us that if we wish to prove $\varphi(\alpha)$ for an arbitrary α , we may assume that $\varphi(\beta)$ holds for $\beta < \alpha$. A proof by this method is called a proof of $\varphi(\alpha)$ by *induction on α* ; the assumption that $\varphi(\beta)$ holds for $\beta < \alpha$ is called the *induction hypothesis*.

We now show that $<$ linearly orders the ordinals, i.e., that

$$\alpha < \beta \vee \alpha = \beta \vee \beta < \alpha. \quad (7)$$

We write (7) as $C(\alpha, \beta)$. We prove $\forall \beta C(\alpha, \beta)$ by induction on α . To prove $\forall \beta C(\alpha, \beta)$, we prove $C(\alpha, \beta)$ by induction on β . Thus we are proving $C(\alpha, \beta)$ using the two induction hypotheses:

$$\forall \gamma < \alpha C(\gamma, \beta), \quad (8)$$

$$\forall \gamma < \beta C(\alpha, \gamma). \quad (9)$$

Now either $\alpha = \beta$ or $\alpha - \beta \neq 0$ or $\beta - \alpha \neq 0$. If $\alpha = \beta$, then $C(\alpha, \beta)$. Now suppose that $\alpha - \beta \neq 0$. By Theorem 5.2 and the definition of $<$, there is a γ such that $\gamma < \alpha$ and $\neg(\gamma < \beta)$. By (8), $C(\gamma, \beta)$, i.e., either $\gamma < \beta$ or $\beta \leq \gamma$. Since the former is false, $\beta \leq \gamma$. Since $\gamma < \alpha$, $\beta < \alpha$ by (6); so $C(\alpha, \beta)$. A similar proof (using (9) instead of (8)) holds if $\beta - \alpha \neq 0$.

Using this, we can prove

$$\alpha \leq \beta \leftrightarrow \alpha \subseteq \beta. \quad (10)$$

For if $\alpha \leq \beta$, $\gamma < \alpha \rightarrow \gamma < \beta$ by (6); so $\alpha \subseteq \beta$ by Theorem 5.2. If $\neg(\alpha \leq \beta)$, then $\beta < \alpha$ by (7) and $\neg(\beta < \beta)$ by (5). Thus $\beta \in \alpha - \beta$; so $\neg(\alpha \subseteq \beta)$. $\square$

We say that α is the *least* ordinal such that $\varphi(\alpha)$ if $\varphi(\alpha)$ holds and $\alpha \leq \beta$ for every β such that $\varphi(\beta)$. There is at most one such α , since $\alpha \leq \beta$ and $\beta \leq \alpha$ imply $\alpha = \beta$ by (5) and (6).

5.4. THEOREM. *If $\exists \alpha \varphi(\alpha)$, then there is a least ordinal α such that $\varphi(\alpha)$.*

PROOF. We suppose that there is no such α and prove $\neg \varphi(\alpha)$ by induction on α . If $\varphi(\beta)$, the induction hypothesis shows that $\neg(\beta < \alpha)$; so $\alpha \leq \beta$. Thus $\neg \varphi(\alpha)$; for otherwise, α would be the least ordinal such that $\varphi(\alpha)$. $\square$

Here are two easy examples of least ordinals: 0 is the least ordinal; $\text{Sc}(\alpha)$ is the least ordinal β such that $\alpha < \beta$.

5.5. THEOREM. *If x is a set of ordinals, then $\text{Un}(x)$ is the least ordinal α such that $\forall \beta \in x (\beta \leq \alpha)$.*

PROOF. The union of a set of transitive sets is transitive; so $\text{Un}(x)$ is transitive. Every member of $\text{Un}(x)$ is a member of some ordinal in x and hence is transitive. Thus $\text{Un}(x)$ is an ordinal. The theorem then follows from (10). $\square$

COROLLARY. *If x is a set of ordinals, there is an ordinal greater than every member of x .*

PROOF. Take $\text{Sc}(\text{Un}(x))$. $\square$

By the Corollary, there is an ordinal which is not a natural number. The least such ordinal is designated by ω . Since $\omega \neq 0$ and 0 is the least ordinal,

$$0 < \omega. \quad (11)$$

Also

$$\alpha < \omega \rightarrow \text{Sc}(\alpha) < \omega. \quad (12)$$

For if $\alpha < \omega$, then $\text{Sc}(\alpha) \leq \omega$ because $\text{Sc}(\alpha)$ is the least ordinal greater than α . Since $\alpha < \omega$, α is a natural number; so $\text{Sc}(\alpha)$ is a natural number; so $\text{Sc}(\alpha) \neq \omega$.

From (11) and (12), every natural number is less than ω and hence belongs to ω . But everything in ω is an ordinal less than ω and hence a natural number. Thus ω is just the set of natural numbers.

Now we turn to definitions of operations by induction. The idea is that we wish to define $F(\alpha)$ in terms of α and the $F(\beta)$ for $\beta < \alpha$. All of these $F(\beta)$ can be combined into a single object $F \upharpoonright \alpha$ defined by

$$F \upharpoonright \alpha = \{\langle F(\beta), \beta \rangle : \beta < \alpha\}.$$

5.6. THEOREM. *If G is a binary operation, then there is a unary operation F such that $F(\alpha) = G(\alpha, F \upharpoonright \alpha)$ for all α .*

PROOF. By an α -function, we shall mean a function f with domain α such that $f(\beta) = G(\beta, f \upharpoonright \beta)$ for all $\beta < \alpha$. It is easy to see that if f is an α -function and $\beta < \alpha$, that $f \upharpoonright \beta$ is a β -function.

We show that there is at most one α -function. For this, we assume that f and g are α -functions and prove

$$\beta < \alpha \rightarrow f(\beta) = g(\beta)$$

by induction on β . If $\gamma < \beta$, then $f(\gamma) = g(\gamma)$ by the induction hypothesis. Thus $f \upharpoonright \beta = g \upharpoonright \beta$; so

$$f(\beta) = G(\beta, f \upharpoonright \beta) = G(\beta, g \upharpoonright \beta) = g(\beta).$$

If there is an α -function f , we set $F(\alpha) = G(\alpha, f)$; otherwise, we set $F(\alpha) = 0$. (It turns out that this otherwise never occurs.)

We first show that $F(\alpha) = G(\alpha, F \upharpoonright \alpha)$ holds if there is an α -function. If f is the α -function, it is enough to show that $F \upharpoonright \alpha = f$. If $\beta < \alpha$, then $f \upharpoonright \beta$ is a β -function; so $F(\beta) = G(\beta, f \upharpoonright \beta) = f(\beta)$ because f is a β -function. Thus $F \upharpoonright \alpha = f$.

It remains to show that there is an α -function for each α . We show that $F \upharpoonright \alpha$ is an α -function by induction on α . Let $f = F \upharpoonright \alpha$. If $\beta < \alpha$, the induction hypothesis and the previous paragraph show that $F(\beta) = G(\beta, F \upharpoonright \beta)$. This is equivalent to $f(\beta) = G(\beta, f \upharpoonright \beta)$, which is what we want. $\square$

In practice, Theorem 5.6 justifies any sort of definition in which $F(\alpha)$ is given in terms of α and the $F(\beta)$ for $\beta < \alpha$. For example, let x be a set and define $F(\alpha)$ to be $\{x\}$ if $\alpha = 0$, $\text{Un}(F(\beta))$ if $\alpha = \text{Sc}(\beta)$, and $\text{Un}\{F(\beta) : \beta < \alpha\}$ otherwise. We easily find a G so that Theorem 5.6 gives this F . The importance of this example is that $F(\omega)$ is a transitive set containing x . For by (11) and (12), $F(\omega)$ is the union of the $F(\alpha)$ for $\alpha < \omega$. In particular, $F(0) \subseteq F(\omega)$; so $x \in F(\omega)$. If $y \in F(\omega)$, then $y \in F(\alpha)$ for some $\alpha < \omega$. Then $y \subseteq \text{Un}(F(\alpha)) = F(\text{Sc}(\alpha)) \subseteq F(\omega)$ by (12). Thus $F(\omega)$ is transitive.

5.7. THEOREM. *If $\forall x (\forall y \in x \varphi(y) \rightarrow \varphi(x))$, then $\forall x \varphi(x)$.*

PROOF. We suppose that the hypothesis holds and that $\neg \varphi(z)$, and derive a contradiction. Using the above, select a transitive set w containing z , and set $v = \{x : x \in w \wedge \neg \varphi(x)\}$. Since $z \in v$, v has a minimal member x . If $y \in x$, then $y \in w$ (because w is transitive) and $y \notin v$; so $\varphi(y)$. By the hypothesis, we have $\varphi(x)$, contradicting $x \in v$. $\square$

Theorem 5.7 tells us that if we wish to prove $\varphi(x)$ for an arbitrary x , we can assume that $\varphi(y)$ holds for all $y \in x$. A proof by this method is called a proof of $\varphi(x)$ by $\in$ -induction on x ; the assumption that $\varphi(y)$ holds for all $y \in x$ is called the *induction hypothesis*.

We now identify the stages with the ordinals and identify the relation *before* with $<$. We say that a set x is formed at the stage α if $x \subseteq R(\alpha)$, where the operation R is defined by induction as follows:

$$R(\alpha) = \text{Un}\{\mathcal{P}(R(\beta)): \beta < \alpha\}.$$

We have thus defined the concepts of Section 2 in ZFC. We now proceed to prove the appropriate properties of these concepts.

By the definition of R ,

$$y \in R(\alpha) \leftrightarrow \exists \beta < \alpha (y \subseteq R(\beta)); \quad (13)$$

i.e., y is in $R(\alpha)$ iff it is formed before α . It follows that x is formed at α iff every member of x is formed before α . This is the first basic property of set formation.

Next, we must show that if every member of a collection is formed before α , then the collection is a set. By (13), this is expressed by

$$\forall x (\varphi(x) \rightarrow x \in R(\alpha)) \rightarrow \text{Set}\{x: \varphi(x)\}.$$

This follows from the Separation Axiom.

Finally, we must show that every set is formed at some stage, i.e.,

$$\exists \alpha (x \subseteq R(\alpha)). \quad (14)$$

We prove this by $\in$ -induction on x . Let $F(y)$ be the least β such that $y \subseteq R(\beta)$, or 0 if there is no such β . Using the Corollary to Theorem 5.5, choose α greater than every ordinal in $\{F(y): y \in x\}$. If $y \in x$ and $\beta = F(y)$, then $y \subseteq R(\beta)$ by the induction hypothesis and $\beta < \alpha$. Thus $y \in R(\alpha)$ by (13). We have proved that $x \subseteq R(\alpha)$.

Putting $\{x\}$ for x in (14), we see that every set belongs to an $R(\alpha)$. This fact is often useful. For example, we can define an operation F on all sets by defining it on each $R(\alpha)$, using induction on α . Another use will be mentioned in the next section. Thus we see that stages are useful in proving theorems as well as in justifying axioms.

6. The Axiom of Choice

A *choice function* on x is a function f with domain $x - \{0\}$ such that $f(y) \in y$ for all y in the domain of f . The Axiom of Choice says that for every set x , there is a choice function on x . (More precisely, the Axiom of Choice is the translation of that sentence into the language of set theory.)

Why is the Axiom of Choice true? We already know that $\text{Un}(x) \times x$ is a set and hence is formed at some stage S . Then every pair $\langle z, y \rangle$ with $z \in y \wedge y \in x$ is formed before S . At stage S , we can pick one such $\langle z, y \rangle$ for each y in $x - \{0\}$ and form the set of these $\langle z, y \rangle$. This set will be a choice function on x .

There is one difficulty in this argument: what do we mean when we say we can pick one $\langle z, y \rangle$ for each y ? Obviously we do not mean that a person can actually pick these pairs, since there may be infinitely many of them. Nor do we mean that there is a rule for picking them; for no matter how we interpret the word *rule*, we can think of no reason why such a rule should exist for every set x . Thus all we can mean is that there is a collection of sets which contains exactly one pair $\langle z, y \rangle$ for each y . If we interpret a collection as being an arbitrary division of the objects available into members and non-members of the collection, it is reasonable to claim that such a collection exists.

The Axiom of Choice has many applications in mathematics, some of which are discussed in Chapter B.2. In set theory, the most interesting applications are to cardinals; so we shall give a brief introduction to cardinals.

We say that x and y are *equinumerous*, and write $x \sim y$, if there is a one-one mapping of x onto y . It is trivial to verify that this is an equivalence relation. We want to associate with each set x a set $|x|$, called the *cardinal of x* , so that

$$|x| = |y| \leftrightarrow x \sim y. \quad (15)$$

The first thought is to use equivalence classes, i.e., to set $|x| = \{y : y \sim x\}$. This will not work because $\{y : y \sim x\}$ is not a set. A solution suggested by the last section is to set $|x| = \{y : y \in R(\alpha) \wedge y \sim x\}$, where α is the least ordinal such that $\exists y \in R(\alpha) (y \sim x)$. (This exists, since $x \sim x$ and x belongs to some $R(\alpha)$.) While this works perfectly well, there is another solution which works even better. We define $|x|$ to be the least ordinal equinumerous with x . First, however, we must prove that there is such an ordinal.

6.1. THEOREM. *If f is a choice function on $\mathcal{P}(x)$, then there is a one-one mapping g of an ordinal α onto x such that for all $\beta < \alpha$, $g(\beta) = f(x - \{g(\gamma) : \gamma < \beta\})$.*

PROOF. Define F by induction as follows:

$$F(\alpha) = f(x - \{F(\beta) : \beta < \alpha\}).$$

(Here $f(0)$ can be taken to be any set, say $\emptyset$.) Then

$$\begin{aligned} x - \{F(\beta) : \beta < \alpha\} &\neq \emptyset \\ \rightarrow F(\alpha) \in x \wedge \forall \beta < \alpha (F(\beta) \neq F(\alpha)). \end{aligned} \quad (16)$$

We first show that $x \subseteq \{F(\beta): \beta < \alpha\}$ for some α . If not, (16) shows that F maps the ordinals one-one into x . The inverse of F then maps some subset of x onto the collection of all ordinals; so this collection is a set by the Replacement Axiom. This contradicts the Corollary to Theorem 5.5.

Let α be the least ordinal such that $x \subseteq \{F(\beta): \beta < \alpha\}$. By (16), $F \upharpoonright \alpha$ maps α one-one onto x and hence is the required g . $\square$

We are thus justified in defining $|x|$ to be the least ordinal equinumerous with x . As remarked, $|x|$ is called the *cardinal* of x . A set is a *cardinal* if it is the cardinal of some set. Every cardinal is an ordinal; and an ordinal α is a cardinal iff $\alpha = |\alpha|$.

We are now going to examine the $\leq$ relation on cardinals. We first prove

$$x \subseteq \delta \rightarrow |x| \leq \delta. \quad (17)$$

Define a choice function f on $\mathcal{P}(x)$ as follows: if $y \in \mathcal{P}(x) - \{0\}$, let $f(y)$ be the least ordinal in y . Let g and α be as in Theorem 5.1. It is easy to check that

$$\beta < \gamma \rightarrow g(\beta) < g(\gamma). \quad (18)$$

We prove

$$\beta < \alpha \rightarrow \beta \leq g(\beta) \quad (19)$$

by induction on β . Assume that $\beta < \alpha$ but $g(\beta) < \beta$. By (18), $g(g(\beta)) < g(\beta)$. But since $g(\beta) < \beta$, the induction hypothesis gives $g(\beta) \leq g(g(\beta))$. This contradiction proves (19).

Now we complete the proof of (17). Suppose $\delta < |x|$. Clearly $|x| \leq \alpha$; so $\delta < \alpha$ and hence $\delta \leq g(\delta)$ by (19). But $g(\delta) \in x$, so $g(\delta) \in \delta$, i.e., $g(\delta) < \delta$. Thus we have a contradiction.

6.2. THEOREM. *If α and β are cardinals, then $\alpha \leq \beta$ iff there is a set having cardinal β which has a subset having cardinal α .*

PROOF. If $\alpha \leq \beta$, then $\alpha \subseteq \beta$ by (10). Since $|\alpha| = \alpha$ and $|\beta| = \beta$, β is the desired set. Now suppose that $|x| = \alpha$, $|y| = \beta$, $x \subseteq y$. There is a one-one mapping of y onto β ; it maps x onto a subset z of β . Thus $\alpha = |x| = |z| \leq \beta$ by (17). $\square$

It is fairly easy to show that every natural number is a cardinal and that ω is a cardinal. Further cardinals can be obtained by the next theorem.

6.3. THEOREM. *For all x , $|x| < |\mathcal{P}(x)|$.*

PROOF. There is a one-one mapping of x into $\mathcal{P}(x)$ which maps y into $\{y\}$. Thus $|x| \leq |\mathcal{P}(x)|$ by Theorem 6.2. We assume that $|x| = |\mathcal{P}(x)|$ and derive a contradiction. By (15), there is a one-one mapping f of x onto $\mathcal{P}(x)$. Let $y = \{z: z \in x \wedge z \notin f(z)\}$. Then $y = f(w)$ for some w . Thus

$$w \in y \leftrightarrow w \notin f(w) \leftrightarrow w \notin y,$$

a contradiction. $\square$

This brief treatment will give the flavor of cardinal theory, but it may not make evident the crucial role of the Axiom of Choice. If we did not have this axiom, we could define cardinals by the first method mentioned above. We could then define $\alpha \leq \beta$ (for α and β cardinals) to mean that there is a set having cardinal β which has a subset having cardinal α . We would not then be able to prove that

$$\alpha \leq \beta \vee \beta \leq \alpha$$

for any two cardinals α and β without the Axiom of Choice.

We conclude this section by showing how Zorn's Lemma is proved from the Axiom of Choice. Recall that a partially ordered set x is *inductively ordered* if every linearly ordered subset of x has an upper bound. Zorn's Lemma says that every inductively ordered set x has a maximal element.

To prove this, we let f be a choice function on $\mathcal{P}(x)$. We define an operation F by induction as follows. Let x_α be the set of all y in x such that $F(\beta) < y$ for all $\beta < \alpha$. Let $F(\alpha) = f(x_\alpha)$ if $x_\alpha \neq 0$, and $F(\alpha) = 0$ if $x_\alpha = 0$. Just as in the proof of Theorem 6.1, we show that $x_\alpha = 0$ for some α . Choose the least such α . If $\gamma < \beta < \alpha$, then $F(\gamma) < F(\beta)$ by the choice of $F(\beta)$; so $\{F(\beta): \beta < \alpha\}$ is linearly ordered. It thus has an upper bound y ; and y is a maximal element because any larger element would be in x_α .

7. Classes

We have noted that certain collections of sets which are not sets can nevertheless be discussed in the language of set theory. We shall now consider this in more detail.

Henceforth, $\{x: \varphi(x)\}$ represents the collection of all sets x such that $\varphi(x)$, even if that collection is not a set. Such a collection is called a class. More precisely, if each variable of $\varphi(x)$ other than x is assigned a set as its

meaning, then $\{x: \varphi(x)\}$ represents a definite collection; and any such collection is called a *class*.

Every set y is a class; for $y = \{x: x \in y\}$. However, not every class is a set. For example, the Russell paradox shows that $\{x: x \notin x\}$ is not a set, and the Corollary to Theorem 5.5 shows that the collection of all ordinals (which is clearly a class) is not a set. A class which is not set is called a *proper* class.

We want $\{x: \varphi(x)\}$ to be a defined symbol; that is, we want every context containing it to be an abbreviation for an expression in the language of set theory. With the new meaning of $\{x: \varphi(x)\}$, we cannot do this by the method of Section 4. Instead, we must examine the contexts in which $\{x: \varphi(x)\}$ may appear.

We wish to allow the expression $\{x: \varphi(x)\}$ to appear immediately before or after $\in$ or $=$. The case in which it occurs immediately after $\in$ is taken care of by the definition

$$y \in \{x: \varphi(x)\} \leftrightarrow \varphi(y).$$

Before proceeding, we introduce some notation. A *term* is an expression which is either a variable or of the form $\{x: \varphi(x)\}$. We use A , B and C to represent terms.

The case in which $\{x: \varphi(x)\}$ occurs immediately before or after $=$ is taken care of by the definition

$$A = B \leftrightarrow \forall x (x \in A \leftrightarrow x \in B). \quad (20)$$

The contexts $x \in A$ and $x \in B$ on the right are taken care of by the previous definition.

Strictly speaking, (20) is a definition only when at least one of A and B is not a variable; for if they are both variables, then $A = B$ is already an expression of the language of set theory. However, (20) is still true in this case, as the Extensionality Axiom shows.

Finally, we take care of the case in which $\{x: \varphi(x)\}$ immediately precedes $\in$ by the definition

$$\{x: \varphi(x)\} \in B \leftrightarrow \exists y (y = \{x: \varphi(x)\} \wedge y \in B).$$

Thus $\{x: \varphi(x)\} \in B$ cannot be true unless $\{x: \varphi(x)\}$ is a set. This is what we would expect; every member of a class is a set.

One technical point must be taken care of. Since $=$ between terms is now defined rather than a logical symbol, the properties of $=$ must be proved rather than covered by logical axioms. This proof is a bit tedious

but without difficulties; it requires the Extensionality Axiom, but no other axioms of set theory.

A useful class is the class of all sets, defined by

$$V = \{x: x = x\}.$$

Note that $A \in V$ is a way of saying that A is a set. In particular, $\{x: \varphi(x)\} \in V$ can replace our previous notation $\text{Set}\{x: \varphi(x)\}$.

A word of caution is necessary. We can now use $\{x: \varphi(x)\}$ without first proving that it is a set. We pay for this by being unable to conclude $\psi(\{x: \varphi(x)\})$ when we have proved $\forall y \psi(y)$. Since $\forall y$ means for all *sets* y , we must first prove that $\{x: \varphi(x)\}$ is a set.

In defining the operations and notions of set theory, it is natural to extend them to classes. Thus we can now define

$$A \cap B = \{x: x \in A \wedge x \in B\}.$$

However, some caution is needed. We can define $\{A\} = \{x: x = A\}$; but if A is a proper class, then $\{A\}$ is the empty set (since no set x is equal to A).

If we are dealing with classes, it is natural to let relations and functions be classes (instead of just sets) of ordered pairs. In particular, the operations of set theory (as applied to sets) may be thought of as functions. For example, the operation $\cup$ becomes the class of all $\langle x, \langle y, z \rangle \rangle$ with $x = y \cup z$. (This class is easily seen to be proper.)

At this point, it is easy to say anything we want about a particular class. However, no formula of the language of set theory says anything about all classes. We indicate by two examples why this is not a great difficulty.

The first example is the simplest property of equality: every class is equal to itself. To show this, we must prove $A = A$ for an arbitrary term A . For this, we note that by (20), $A = A$ is equivalent to $\forall x (x \in A \leftrightarrow x \in A)$, and the latter follows from the laws of logic.

This simple example illustrates the general procedure. We prove that something is true of all classes by proving $\varphi(A)$ for an arbitrary term A . In doing so, we are not proving one formula of the language of set theory, but infinitely many formulas, one for each choice of A . This is usually immaterial, since with rare exceptions the proof is the same for all A .

Things are a bit more complicated when we wish to state that a class exists. This is illustrated when to try to reformulate Theorem 5.6 to talk about classes instead of operations. Let $\varphi(A, B)$ result from translating the following into the language of set theory: if A is a function with domain $V \times V$, then B is a function with domain the class of ordinals such that $B(\alpha) = A(\alpha, F \upharpoonright \alpha)$ for all α . Then the theorem in question is intuitively

expressed by $\forall A \exists B \varphi(A, B)$. But this is not a formula of the language of set theory in any sense, since terms other than variables cannot appear after quantifiers.

What can it mean to prove $\forall A \exists B \varphi(A, B)$ in ZFC? An examination of the proof we gave of Theorem 5.6 gives the answer. What we must do is show how, given any term A , we can produce a term B and then prove $\varphi(A, B)$ in ZFC.

These procedures enable us to handle all the statements we wish to make about classes. There is another possible procedure: we can extend the language by introducing variables for classes and allowing these variables to appear after quantifiers. This gives a simpler and more straightforward solution to the sort of problem we have been discussing. There is a penalty, however; the added notation makes added work when it comes time to do independence proofs. On the whole, the recent tendency has been to stick to the language of set theory and use the methods described in this section.

8. New axioms

The most important discovery in set theory in recent years is that many of the important unsolved problems of set theory cannot be settled from the axioms of ZFC. Among these are the Continuum Hypothesis and the Souslin problem. We are thus led to seek new axioms which solve these problems. We will try to give the reader an idea of what has been done and what remains to be done.

Where shall we look for new axioms? One idea is suggested by Section 4. We found there two principles of the form: every *collection* of sets satisfying certain conditions is a set. When we came to formulating these principles as axioms in the language of set theory, we could only say that every *class* satisfying the conditions was a set. That this is not a trivial point is shown by the models used in independence proofs. In these models, there is always a set belonging to the model which has a subset which does not belong to the model.

Unfortunately, it is not easy to deal with collections which are not classes. Consider, for example, a simple-minded approach: we add new variables which represent arbitrary collections. It is now easy to write axioms which say that every collection having a certain property is a set. We cannot use such axioms, however, until we have axioms telling us that there are collections. The obvious such axioms say that every class is a collection. When we have introduced these axioms, we are right back where we started from.

A better idea is to introduce into the language symbols for new operations on sets, so that there are more collections of the form $\{x: \varphi(x)\}$. Of course these operations must be really new; i.e., they must not be definable in the language of set theory. Now very few such operations are known, and introducing the known ones does not solve any of the open problems of set theory. Thus at present, we can do nothing with this approach.

The solution to making use of arbitrary collections may lie in a different direction. If $\varphi(x)$ is a formula in some reasonable language, we may think of $\varphi(x)$ as providing a rule for determining which sets belong to $\{x: \varphi(x)\}$. Now as we noted in discussing the Axiom of Choice, there is no reason why a collection should have such a rule. If we could further analyze the notion of a collection not formed according to a rule, we might arrive at axioms other than the Axiom of Choice which utilize such collections, or at least find a more convincing argument for the truth of the Axiom of Choice.

There is another approach to finding new axioms which has been more successful. Recall that in Section 3, we formulated a vague principle on the existence of stages and derived three precise principles from it. If we could derive further precise principles, we could hope to obtain new axioms.

The vague principle asserts the existence of stages which are after many other stages. Thus in view of the identifications of Section 5, we can expect the new axioms to state that there are ordinals which are very large. Since these ordinals generally turn out to be cardinals, the axioms are called *large cardinal axioms*. Much work has been done with such axioms; we are only going to indicate the direction this work has taken. See also Section 7 of Chapter B.3 and its anonymous Appendix.

Let S be the collection of all stages which can be obtained by the three precise principles of Section 3. Clearly the weakest new precise principle would be: there is a stage which is after every stage in S . To justify this by our vague principle, we must be able to imagine a situation in which all the stages in S are completed, i.e., in which the three principles of Section 3 lead to no new stages. Without some sort of further analysis, it is not clear whether we can do this. (We thus begin to see the weakness of the vague principle.) However, let us suppose that our imagination is strong enough for the task, and see what new axiom results.

Our axiom should state that there is an α so large that if the three principles of Section 3 are applied to ordinals before α and sets formed before α , the resulting ordinals are less than α . For the third principle, this means that if $x \in R(\alpha)$ and f is a mapping of x into α , then $\text{Un}(\text{range}(f)) < \alpha$ (see Theorem 5.5). Now if we assume $\omega < \alpha$, then $\omega \in R(\alpha)$; so this

implies that if y is a countable set of ordinals less than α , then $\text{Un}(y) < \alpha$. This implies that the first two principles of Section 3 lead only to ordinals less than α .

We are thus led to the following definition: α is *inaccessible* if $\omega < \alpha$ and if whenever f is a mapping of a set in $R(\alpha)$ into α , then $\text{Un}(\text{range}(f)) < \alpha$. It is easy to show that every inaccessible ordinal is a cardinal, and that our definition of an inaccessible cardinal is equivalent to the one usually given.

Our first large cardinal axiom states that there is an inaccessible cardinal. The first thing to show is that it really is a new axiom, i.e., that it is not provable in ZFC. We sketch how this is done.

What we need is a model of ZFC in which the new axiom is false. Now if there is no inaccessible cardinal, the class of all sets furnishes such a model. Now suppose that α is the least inaccessible cardinal. Since α and $R(\alpha)$ satisfy the three principles of Section 3, we suspect that $R(\alpha)$ is a model of ZFC. This is indeed the case; the proof rather resembles our derivation of the axioms of ZFC from the principles of Section 3. The fact that the new axiom does not hold in $R(\alpha)$ follows (with some work) from the fact that there is no inaccessible cardinal in $R(\alpha)$.

Does the new axiom have any interesting consequences? There is at least one. A famous theorem of Gödel says that the consistency of ZFC cannot be proved in ZFC. This consistency can be proved from the new axiom. The crucial fact has already been stated: if α is inaccessible, then $R(\alpha)$ is a model of ZFC. Once we have a set which is a model of ZFC, it is easy to prove that ZFC is consistent.

On the other hand, our axiom contributes nothing to the unsolved problems mentioned at the beginning of this section; for the independence proofs remain correct when we introduce the new axiom. Thus we must look for stronger large cardinal axioms.

We shall consider one such axiom, which says that a measurable cardinal exists. We shall not give the precise definition of a measurable cardinal. Suffice it to say that nothing about the definition suggests that a measurable cardinal must be large. However, we can prove that measurable cardinals are inaccessible, and that they are, in certain senses, much larger than inaccessible cardinals. For example, if α is a measurable cardinal, then there are α inaccessible cardinals less than α .

What we would really like to do (but are presently unable to do) is to reformulate the definition of a measurable cardinal to look like this: α is measurable iff α and $R(\alpha)$ are closed under certain operations. We could then try to justify the existence of a measurable cardinal by imagining a situation in which these operations produce no new ordinals.

We thus see that there is much less reason to believe in the existence of a measurable cardinal than in the existence of an inaccessible cardinal. On the other hand, the former assumption solves various interesting problems in set theory. We mention one result which is likely to interest mathematicians. If there is a measurable cardinal, then every set of real numbers which is the continuous image of the complement of a continuous image of a Borel set is measurable. It is certainly surprising that the existence of a large cardinal implies the measurability of a set of real numbers.

We mention here one further axiom (not a large cardinal axiom): the Axiom of Projective Determinacy. This axiom solves a great many more problems than the existence of a measurable cardinal. On the other hand, there is no reason for believing that this axiom is true, except that it is an elegant axiom with interesting consequences.

Thus we see that the more problems a new axiom settles, the less reason we have for believing the axiom is true. Moreover, we have no good axioms at all which settle the most important unsolved problem, the Continuum Hypothesis. We are therefore very far from the goal of solving our problems by means of new axioms. Nevertheless, there is no reason to be discouraged. If the rather elementary analysis of Section 3 leads us as far as it did, there is reason to hope that a deeper analysis will lead to new axioms with profound consequences.

About the Axiom of Choice

THOMAS J. JECH

Contents

1. Introduction	346
2. Do we need the axiom of choice?	348
3. The “paradoxical” decomposition of a ball.	351
4. Some uses of the axiom of choice	354
5. Consistency of the axiom of choice	358
6. Independence of the axiom of choice	359
7. Transfer theorems	363
8. Mathematics without the axiom of choice	365
9. Definable choice	368
10. Determinacy — an alternative to the axiom of choice.	369
References.	370

1. Introduction

I guess I may assume that the reader has heard about the axiom of choice and possibly has even seen a proof of some theorem which makes use of the axiom of choice

The statement of the axiom of choice is very simple and easy to arguments about the foundations of mathematics.

1.1. AXIOM (see Fig. 1). *Let $\mathcal{F} = \{A_i : i \in I\}$ be a collection of pairwise disjoint nonempty sets. There exists a set $C = \{x_i : i \in I\}$ which has exactly one element x_i common with each $A_i \in \mathcal{F}$.*

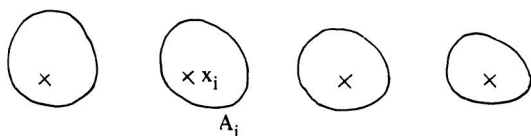


Fig. 1.

Now why has this simple (if not self-evident) axiom generated so much controversy? For no postulate since Euclid's Parallel Axiom aroused so much excitement in mathematical circles and led to so many philosophical arguments about the foundations of mathematics.

The answer lies in the nonconstructive nature of the axiom of choice. The axiom postulates existence of a set C which has certain properties (namely *chooses* one element x_i in each A_i), but does not give the slightest hint how to construct such a set. On the other hand, all other axioms of set theory assert that certain constructions on sets result in new sets, and that various totalities of elements, defined in a certain way, are indeed sets. For instance, the power set axiom states that for every set X , the collection $\mathcal{P}(X)$ of all subsets of X is a set.

In case that the reader does not consider this distinction too important, I would like to remind him, that traditionally, until the late nineteenth century, existence in mathematics was synonymous with construction. Cantor's alternate proof of existence of transcendental numbers, or Hilbert's solution of Gordan's problem met with a skeptical reaction and even animosity of leading mathematicians of that time. (The tendency to emphasize constructions was even stronger in the mathematical public: a Professor Hermes devoted ten years of his life to the construction of a regular polygon of 65,537 sides, which had been proved to be possible by Gauss a century earlier.)

The explicit formulation of the axiom of choice is usually ascribed to Zermelo. According to FRAENKEL, BAR-HILLEL and LÉVY [1973] (which gives an excellent account of not only the axiom of choice but of the whole axiomatic foundations of set theory) the first explicit allusion to the principle of choice was made by Peano in an 1890 paper on differential equations, although Cantor had inadvertently applied the axiom before.

In 1904, Zermelo gave a proof that every set can be well-ordered (a linear ordering $<$ of a set S is a *well-ordering* if every nonempty subset X of S has a least element). Earlier, when Cantor invented the theory of cardinal numbers, he posed the problem to determine the size of the continuum (the *continuum hypothesis*) and made the assumption that the set of all real numbers (the continuum) can be well-ordered, or, what amounts to the same, that it can be arranged into a transfinite sequence. Needless to say that since no such well-ordering had been constructed, this assumption met with a strong opposition.

To prove that *every* set can be well-ordered, Zermelo formulated the axiom of choice, more or less in the same form as it is used today. In our terminology the principle is thus stated as follows:

1.2. AXIOM OF CHOICE. *For every family $\mathcal{F}$ of nonempty sets, there exists a function f such that $f(S) \in S$ for each set S in the family $\mathcal{F}$.*

The function f is called a *choice function* on $\mathcal{F}$. Before taking a look at Zermelo's proof, let me show that the formulation 1.2 is equivalent to the first formulation 1.1. In fact, 1.1 is a special case of 1.2: if the family $\mathcal{F}$ consists of pairwise disjoint sets then 1.1 and 1.2 clearly say the same thing. Thus let us show that if we assume the choice principle for disjoint collections of sets, we can prove the general form 1.2.

Let $\mathcal{F}$ be a family of nonempty sets: $\mathcal{F} = \{X : X \in \mathcal{F}\}$. To apply 1.1, we employ the following trick to "make the sets in $\mathcal{F}$ disjoint": For each $X \in \mathcal{F}$, let S_X be the set of all ordered pairs (X, a) , where $a \in X$:

$$S_X = \{X\} \times X.$$

Now, the collection $\{S_X : X \in \mathcal{F}\}$ consists of pairwise disjoint nonempty sets, and using 1.1, we can pick one element z_X from each S_X . Since for each $X \in \mathcal{F}$, z_X has the form (X, a_X) where $a_X \in X$, it is easy to see that we obtain a choice function f on $\mathcal{F}$: we let $f(X) = a_X$ for each $X \in \mathcal{F}$.

Now back to Zermelo. The proof of the well-ordering theorem goes

roughly as follows: Let S be an arbitrary set; we wish to find a well-ordering of S . Using the axiom of choice, we assume that there exists a choice function f on the family $\mathcal{F}$ of all nonempty subsets of S . By transfinite induction one constructs a transfinite sequence $\langle a_\alpha : \alpha < \theta \rangle$ in S as follows: having constructed the first α terms of the sequence, $a_0, a_1, \dots, a_\xi, \dots$ ($\xi < \alpha$), one looks whether there are any elements of S left; whether the set $X = S - \{a_\xi : \xi < \alpha\}$ is nonempty. If it is nonempty, one chooses a_α by means of the choice function f : $a_\alpha = f(X)$. This procedure is continued until for some ordinal number θ , the set $S - \{a_\xi : \xi < \theta\}$ is empty; in other words, $S = \{a_\xi : \xi < \theta\}$. Such enumeration of S by ordinal numbers gives a well-ordering of S .

Now you can see that although we proved Cantor's assumption that the continuum can be well-ordered, we have not produced any well-ordering of the reals that one could lay hands on; we have just replaced one dubious assumption by another dubious assumption, namely by the axiom of choice.

In fact, the axiom of choice and Zermelo's well-ordering theorem are logically equivalent. Let me show how the axiom of choice follows from the assumption that every set can be well-ordered: Let $\mathcal{F}$ be a family of nonempty sets. We let S be the union of the family $\mathcal{F}$: $S = \bigcup \{X : X \in \mathcal{F}\}$. Using a well-ordering $<$ of S , we define a choice function f on $\mathcal{F}$ as follows: if $X \in \mathcal{F}$, we let $f(X)$ be the least element of X in the ordering $<$.

2. Do we need the axiom of choice?

That of course depends on what kind of mathematics we are engaged in. If you are solving differential equations, foliating manifolds or investigating groups of large but finite order, you will probably never encounter a problem having anything to do with the axiom of choice. However, a large part of present day mathematics deals with abstract infinite structures and in many areas, mathematicians are more and more concerned with the foundations of mathematics. And the axiom of choice is indispensable not only in logic (set theory and model theory) but in other modern disciplines as well: point set topology, algebra, functional analysis, measure theory.

To illustrate the use of the axiom of choice, let me consider some banality like the following: Everyone knows that the union of countably many countable sets is countable. This is used in real analysis all over and most people do not even realize that the proof uses the axiom of choice. After all, the proof goes like this:

$$\begin{array}{ccccccc}
 A_0 & a_{00} & a_{01} & a_{02} & \cdots & a_{0n} & \cdots \\
 A_1 & a_{10} & a_{11} & a_{12} & \cdots & a_{1n} & \cdots \\
 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 & & & & & & \\
 A_m & a_{m0} & a_{m1} & a_{m2} & \cdots & a_{mn} & \cdots \\
 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
 \end{array} \tag{1}$$

We are given countably many sets $A_0, A_1, \dots, A_m, \dots$ and each A_m is countable, thus $A_m = \{a_{mn}\}_{n=0}^\infty$. Hence we can arrange the elements of the union $A = \bigcup_{m=0}^\infty A_m$ into a countable sequence using the well known counting method:

$$a_{00}, a_{01}, a_{11}, a_{10}, a_{02}, a_{12}, a_{22}, a_{21}, a_{20}, \dots$$

So where is the axiom of choice?

Let me go over the proof once more. We are given a countable collection of sets $\mathcal{A}$; hence we can enumerate the elements of $\mathcal{A}$ by integers and have

$$\mathcal{A} = \{A_0, A_1, \dots, A_m, \dots\}_{m=0}^\infty.$$

Each A_m is a countable set and so for each m , there exists an enumeration of elements of A_m by integers

$$A_m = \{a_{m0}, a_{m1}, \dots, a_{mn}, \dots\}_{n=0}^\infty. \tag{2}$$

However, there exists more than one enumeration of the set A_m . If E_m denotes, for each m , the set of all enumerations of A_m (of the form (2)), we are confronted with the following problem: if we want to apply the diagram (1), we have to *choose* one specific enumeration of A_m , for each m . In other words, we have to choose one element from each set E_m . And here we are: we need a choice function on the family $\{E_0, E_1, \dots, E_m, \dots\}_{m=0}^\infty$. Naturally, the argument above shows that the axiom of choice is used in this particular proof of the theorem that the union of countably many countable sets is countable; it does not rule out the possibility of finding an alternate proof that would make no reference to the axiom of choice. However, it has been established (by methods which I shall discuss later in this article) that it is not so; one *cannot* prove without the axiom of choice that the union of countably many countable sets is countable; in fact, one cannot even prove that the set of all real numbers is not the union of countably many countable sets (!).

The need for the axiom of choice becomes stronger as we move away from the continuum into the world of abstract structures and spaces. I shall give below examples of fundamental theorems of abstract algebra and

topology whose proofs use the axiom of choice. In some instances, the theorems are as strong as the axiom of choice: an example of a statement equivalent to the axiom of choice is the Tychonoff product theorem in point set topology.

If we want to use *convenience* as a criterion for accepting the axiom of choice, then its widespread use in many branches of mathematics in the last 50 years speaks clearly in favor of the axiom. On the other hand, admitting that the nonconstructive character of the axiom makes it less self evident than other axioms, we have to ask about its formal *consistency*: does not the addition of the axiom to the other axioms of set theory lead to a contradiction? This has fortunately been settled by Gödel in 1939: the axiom of choice is consistent with the axiomatic set theory. Thirdly, we should not be satisfied with formal consistency of the axiom. If we are to accept it, we should believe in its *plausibility*. We should make sure that the arguments that use the axiom of choice and the results that are obtained with its help are not contrary to our picture of the mathematical universe (I would not insist though too much on this point. After all, mathematics abounds in “counterintuitive” examples. Just look at Weierstrass’ construction of a continuous nondifferentiable function). Finally, again due to the nonconstructive character of the axiom it is interesting to find out whether the use of the axiom of choice in proofs of certain theorems is necessary and to what extent: this raises the questions of *relative strength* of various weaker forms and consequences of the axiom of choice.

I will address myself first to the question of plausibility. At the first glance, the axiom seems to be quite obvious: we are to pick one element $f(S)$ from each set S in a given family $\mathcal{F}$.

In popular expositions, the axiom of choice has been often compared to elections: we may look at each set $S \in \mathcal{F}$ as a list of candidates for a given office and the election process provides a choice function f that determines the elected candidate $f(S)$, for every $S \in \mathcal{F}$.

Of course, this analogy gives a justification of sorts for the finite case of the axiom, when both $\mathcal{F}$ and all $S \in \mathcal{F}$ are finite. And as we know, we cannot apply our intuition based on the finite world indiscriminately to infinite sets. Nevertheless, the axiom of choice is demonstrably true if the family $\mathcal{F}$ is finite, regardless whether the sets $S \in \mathcal{F}$ are finite or not.

This is proved by induction on size of $\mathcal{F}$. If $\mathcal{F}$ consists of one nonempty set S , then any function f whose only argument is S and whose value at S is (any) element a of S is a choice function on $\mathcal{F}$. And that such a function f exists follows simply from the fact that S is nonempty: the latter means that an $a \in S$ exists.

Assuming that the axiom holds for all families of size n , we easily prove that it holds as well for families of size $n + 1$: Let $\mathcal{F} = \{S_1, \dots, S_n, S_{n+1}\}$ be a family of $n + 1$ nonempty sets. By the induction hypothesis, the family $\{S_1, \dots, S_n\}$ has a choice function g . Since S_{n+1} is nonempty, there is some $a \in S_{n+1}$ and hence there is an extension f of g , defined on $\mathcal{F}$, whose value at S_{n+1} is a . Clearly, such function f is a choice function on $\mathcal{F}$.

Another case, in which the axiom of choice is demonstrably true, is when each $S \in \mathcal{F}$ consists of a single element. Then $\mathcal{F}$ has a choice function and, in fact, this choice function is unique. (Thinking again about the analogy with elections I cannot help wondering whether this mathematical problem of existence of a choice function is not the reason why certain countries keep holding elections with exactly one candidate for each office.)

While we have seen that every finite family $\mathcal{F}$ has a choice function, the finiteness of the elements of $\mathcal{F}$ does not generally guarantee that a choice function exists. In some cases, finiteness of the sets $S \in \mathcal{F}$ helps: especially if the sets S are endowed with some internal structure. For instance, if $\mathcal{F}$ is a family of finite sets of real numbers, then a choice function on $\mathcal{F}$ exists: For each $S \in \mathcal{F}$, let $f(S)$ be the least element of S . On the other hand, if $\mathcal{F}$ consists of finite sets of sets of real numbers, then there is no apparent way of finding a choice function on $\mathcal{F}$ (and in fact, the existence of a choice function cannot be proved in this case).

A classical illustration of this point (due to Russell) contrasts the case of an infinite set of pairs of shoes with that of an infinite set of pairs of socks. While the set of pairs of shoes has an obvious choice function (namely, choose the right shoe from each pair), there seems to be no way how to choose (without recourse to the axiom of choice) among two socks, simultaneously for infinitely many pairs.

3. The "paradoxical" decomposition of a ball

Some objections to the axiom of choice were based on the fact that the axiom has paradoxical consequences. Using the axioms, one can obtain results that are in conflict with our intuition. The most famous example is the following paradox.

3.1. BANACH-TARSKI PARADOX. *Using the axiom of choice, one can cut a ball into a finite number of pieces that can be so rearranged that one obtains two balls of the same size as the original ball.*

I will sketch the proof of this “paradox”, to show how the axiom of choice is used, and to show that there is nothing paradoxical about this theorem: The pieces of the ball are just nonmeasurable sets and the construction is not much different from the well-known construction of a nonmeasurable subset of the real line.

Of course the pieces in question cannot be measurable: the theorem would then be in contradiction with additivity of measure. Let me first recall Vitali’s construction of a nonmeasurable set of real numbers: Let us consider the following equivalence relation on real numbers in the interval $[0, 1]$:

$$x \sim y \quad \text{iff} \quad x - y \text{ is a rational number.}$$

This equivalence relation gives us a decomposition of $[0, 1]$ into equivalence classes. Using the axiom of choice, we pick one element from each equivalence class and collect them into a set M . This set $M \subset [0, 1]$ cannot be measurable: For each rational number r , let $M_r = \{x + r : x \in M\}$. By the construction of M , the sets M_r are mutually disjoint and every real number belongs to some (unique) M_r . If M were measurable, each M_r would have the same measure as M . If M were a null set, then all M_r would be too, and the real line would be the union of countably many null sets, which it is not. On the other hand, if M has a positive measure, then the union $\bigcup \{M_r : r \text{ is rational and } 0 \leq r \leq 1\}$ of infinitely many disjoint sets of the same positive measure has to have infinite measure; this is a contradiction since the union is included in the interval $[0, 2]$.

The Banach–Tarski paradox is based on an earlier theorem of Hausdorff that gives a paradoxical decomposition of a sphere:

3.2. THEOREM (HAUSDORFF [1914]). *A sphere S can be decomposed into disjoint sets $S = A \cup B \cup C \cup Q$ such that:*

- (i) *the sets A, B, C are congruent to each other;*
- (ii) *the set $B \cup C$ is congruent to each of the sets A, B, C ; and*
- (iii) *Q is countable.*

I will give a very short sketch of the proof. Some more details are in JECH [1973]; the complete proof can be found in Hausdorff’s book.

Let us consider two axes of rotation a_φ, a_ψ of the sphere, and consider the group of all rotations generated by a rotation φ by 180° about a_φ and a rotation ψ by 120° about a_ψ . All such rotations can be described by formal products (“words”) formed by φ, ψ and ψ^2 , with the specification that $\varphi^2 = 1$ and $\psi^3 = 1$ (this is, if you like, the free product of the groups $\{1, \varphi\}$ and $\{1, \psi, \psi^2\}$).

First I claim that the axes a_φ and a_ψ can be chosen in such a way that distinct "words" describe distinct rotations generated by φ and ψ . To prove the claim, it suffices to determine the angle θ between a_φ and a_ψ so that no nontrivial word describes the identity rotation. If a word does describe the identity rotation, then θ is a solution of a certain equation. It so happens that the equation has only finitely many solutions and it follows that there are only countably many angles θ such that some nontrivial word describes the identity rotation. Hence any angle outside this countable set will do. The key step in the proof is the decomposition of the group G of all words (or rotations generated by φ and ψ) into three disjoint sets $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ such that

$$\mathcal{A} \cdot \varphi = \mathcal{B} \cup \mathcal{C}, \quad \mathcal{A} \cdot \psi = \mathcal{B}, \quad \mathcal{A} \cdot \psi^2 = \mathcal{C}.$$

The construction is not difficult and the reader can probably find such decomposition himself if he cares to try.

Now we use the axiom of choice in a similar way we used it in Vitali's construction. Each rotation $\alpha \in G$ leaves two points of the sphere S fixed; it follows that the set Q of all points on the sphere that are fixed by some rotation $\alpha \in G$ is countable. The set $S - Q$ is the disjoint union of the equivalence classes ("orbits") given by the equivalence relation

$$x \sim y \quad \text{iff} \quad y = x\alpha \quad \text{for some } \alpha \in G.$$

By the axiom of choice, there exists a set M which contains exactly one element in each orbit. If we let

$$A = M \cdot \mathcal{A}, \quad B = M \cdot \mathcal{B}, \quad C = M \cdot \mathcal{C},$$

then the sets A, B, C and Q satisfy the statement of Hausdorff's theorem.

To obtain the Banach-Tarski paradox, let us consider the following equivalence relation between sets in the three-dimensional Euclidean space: $X \approx Y$ iff there is a finite decomposition of X into disjoint sets $X = X_1 \cup \cdots \cup X_m$ and a decomposition of Y into the same number of disjoint sets $Y = Y_1 \cup \cdots \cup Y_m$ such that X_i is congruent to Y_i , for each $i = 1, \dots, m$.

It is easy to verify that $\approx$ is an equivalence and that if X is disjoint from X' , Y is disjoint from Y' , $X \approx Y$ and $X' \approx Y'$, then $X \cup X' \approx Y \cup Y'$. A more important property is that if $X \subseteq Y \subseteq Z$ and $X \approx Z$, then $X \approx Y$. (The proof of this property is like the proof of the Cantor-Bernstein Theorem: If $X \subseteq Y \subseteq Z$ and $|X| = |Z|$, then $|X| = |Y|$.)

Having Hausdorff's decomposition of the sphere at our disposal, it is not too difficult to use the properties of the equivalence relation $\approx$ to prove:

3.3. THEOREM (Banach–Tarski (1924)). *A closed ball U can be decomposed into two disjoint sets*

$$U = X \cup Y$$

such that $U \approx X$ and $U \approx Y$.

4. Some uses of the axiom of choice

In this section I shall discuss some typical applications of the axiom of choice in mathematics. I have already mentioned the Tychonoff product theorem stating that the topological product of any collection of compact spaces is compact. It is not surprising that the product theorem uses the axiom of choice; after all, the statement that the cartesian product of any collection of nonempty sets is nonempty is just another formulation of the axiom of choice. (The elements of a cartesian product are the choice functions.)

In fact the relationship of the Tychonoff theorem and the axiom of choice is even closer: it has been shown by Kelley that the axiom of choice can be proved if one assumes that Tychonoff theorem is true. Thus the two statements are logically equivalent (in set theory without the axiom of choice).

A large number of proofs using the axiom of choice, particularly in algebra, follow a similar pattern. The theorem in question is reduced to a statement asserting existence of a *maximal* object in a certain class of objects. For instance, let us consider the theorem stating that every vector space has a basis. It is rather obvious that a set of vectors is a basis if and only if it is linearly independent and moreover maximal among linearly independent sets (i.e. there is no larger linearly independent set). Thus, to prove the theorem it suffices to show that there exists a maximal independent set.

Another such example is the Hahn–Banach Theorem in functional analysis. One version of the theorem states that any linear functional on a subspace of a given vector space can be extended to a linear functional on the whole space. Again, if one considers the family $\mathcal{F}$ of all extensions of the given functional (whether defined everywhere or not), then those functionals that are defined everywhere in the space are exactly the maximal elements of the family $\mathcal{F}$.

This phenomenon had been recognized and led to the formulation of a general principle, usually referred to as Zorn's lemma (it was first proved by Kuratowski and rediscovered twenty years later by Zorn).

Let $(P, <)$ be a partially ordered set. A subset C of P is called a *chain* in P if it is linearly ordered by $<$. An element $u \in P$ is an *upper bound* of C if $c \leq u$ for every $c \in C$. An element $a \in P$ is a *maximal* element if there exists no $x \in P$ such that $a < x$.

4.1. ZORN'S LEMMA. *Let $(P, <)$ be a nonempty partially ordered set with the property that every chain in P has an upper bound. Then P has a maximal element.*

Let us see how Zorn's lemma can be used in the above examples. In the first example, let P be the collection of all linearly independent subsets of the vector space, and let $X < Y$ just in case $X \subset Y$. A chain in P is a collection C of independent sets such that for any $X, Y \in C$, either $X \subseteq Y$ or $Y \subseteq X$. If C is such a chain then the set $\bigcup\{X: X \in C\}$ is a linearly independent set and is an upper bound of C . Hence $(P, <)$ satisfies the assumption of Zorn's lemma and so has a maximal element B . It follows that B is a basis of the vector space.

The proof of Hahn-Banach Theorem is similar. We let P be the collection of all linear functionals extending the given functional, and let $f < g$ just in case g extends f . It is easily verified that Zorn's lemma is applicable to $(P, <)$, and a maximal element of P is the required extension.

Zorn's lemma is easily proved when we assume the axiom of choice: Let $(P, <)$ be a partially ordered set such that every chain has an upper bound. We construct an increasing transfinite sequence of elements of P : $a_0 < a_1 < \dots < a_\alpha < \dots$. As long as we do not reach a maximal element, we can find a yet bigger element (and can choose one), since every chain has an upper bound. Eventually, we do reach a maximal element.

It is worth noting that vice versa, Zorn's lemma implies the axiom of choice. Let me show how to obtain a choice function on a family $\mathcal{F}$ of nonempty sets, using Zorn's lemma: Let P be the collection of all choice functions on subfamilies of $\mathcal{F}$, and let $f < g$ just in case g extends f . Applying Zorn's lemma, one gets a choice function on $\mathcal{F}$.

I will now discuss one consequence of the axioms of choice which has the remarkable property that there is a number of seemingly unrelated theorems that are all equivalent to it.

I assume that the reader is familiar with the notion of Boolean algebra. A subset I of a Boolean algebra B is an *ideal* if

- (i) $0 \in I$, $1 \notin I$,
- (ii) $a \in I$ and $b \leq a$ implies $b \in I$,
- (iii) if $a \in I$ and $b \in I$, then $a + b \in I$.

An ideal I in B is a *prime ideal* if for every $a \in B$, either $a \in I$ or $-a \in I$.

4.2. PRIME IDEAL THEOREM (Tarski). *Every Boolean algebra has a prime ideal.*

The proof of the prime ideal theorem is a typical application of Zorn's lemma. Once we verify that an ideal in B is prime if and only if it is maximal (among ideals in B), we simply apply Zorn's lemma to the collection of all ideals in B .

Note that the prime ideal theorem readily implies its stronger version: *In a Boolean algebra, every ideal can be extended to a prime ideal.*

For if I is an ideal in B , we consider the quotient algebra B/I and once we get a prime ideal on B/I , we simply take the inverse image of this prime ideal under the natural homomorphism $h : B \rightarrow B/I$.

In the particular case that B is the algebra of all subsets of a given set S , it follows that every ideal over S can be extended to a prime ideal over S . Equivalently, using the dual notions of filter and ultrafilter, it follows that every filter over a set S can be extended to an ultrafilter. (In fact, this statement is equivalent to the prime ideal theorem.)

Once we have this formulation of the prime ideal theorem in terms of ultrafilters it is immediately clear how important the theorem is in point set topology. This is further witnessed by the following fact: The prime ideal theorem is equivalent to the Tychonoff theorem for products of compact Hausdorff spaces.

The prime ideal theorem is also an important tool in logic. For instance, one of the basic principles in model theory is the *Compactness Theorem*: *If every finite subset of a set of sentences Σ has a model, then Σ has a model.* (See 2.4 and 4.2 in Chapter A.1.) It turns out that the Compactness Theorem is equivalent to the prime ideal theorem.

Let me illustrate how the compactness theorem can be used in lieu of the axiom of choice in some proofs. Let us prove that every set can be linearly ordered. (Since the prime ideal theorem is weaker than the axiom of choice, we do not try to prove that every set can be well-ordered.) Let S be an arbitrary set. Let us consider a language that provides a name $\dot{x}$ for each element x of S , and has a binary predicate $<$. Let Σ be the following set of sentences:

$$\left. \begin{array}{l} \dot{x} \not< \dot{x}, \\ \dot{x} < \dot{y} \quad \text{and} \quad \dot{y} < \dot{z} \Rightarrow \dot{x} < \dot{z}, \\ \dot{x} < \dot{y} \quad \text{or} \quad \dot{y} < \dot{x} \quad \text{or} \quad \dot{x} = \dot{y}, \end{array} \right\} \quad \text{for all } x, y, z \in S.$$

Since every finite subset of S can be linearly ordered, it follows that every finite subset of Σ has a model. By the compactness theorem, Σ has a model and this model provides a linear ordering of S .

For those readers that like point set-topological arguments, let me present a sample proof involving a topological version of the prime ideal theorem. The following principle appears quite often, in different situations and under various guises (one version is called the *Rado selection lemma*):

4.3. LEMMA. *Let S be a set, let E be a finite set, and let $\mathcal{F}$ be a collection of functions t such that*

- (i) *$\text{dom}(t)$ is a finite subset of S and $\text{ran}(t) \subseteq E$,*
- (ii) *if $t \in \mathcal{F}$ and $t' \subset t$, then $t' \in \mathcal{F}$,*
- (iii) *for every finite $X \subseteq S$ there is $t \in \mathcal{F}$ such that $X \subset \text{dom}(t)$.*

Then there exists a function $f: S \rightarrow E$ such that for every finite $X \subseteq S$, the restriction $f|X$ belongs to $\mathcal{F}$.

PROOF. To prove this theorem, consider the topological product E^S (where E has the discrete topology). By Tychonoff's theorem for Hausdorff spaces, E^S is compact. For every finite $X \subseteq S$, let $F_X = \{f \in E^S: f|X \in \mathcal{F}\}$. Each F_X is closed, and the collection $\mathcal{C} = \{F_X: X \subseteq S \text{ finite}\}$ has the finite intersection property. Thus the intersection of $\mathcal{C}$ is nonempty and yields an element of $\mathcal{F}$. $\square$

Since the Rado selection lemma can be used in the proof of the compactness theorem, it follows that it is equivalent to the prime ideal theorem.

We note in passing that the Hahn-Banach Theorem is in fact a consequence of the prime ideal theorem; the full axiom of choice is not necessary. Another notable consequence of the prime ideal theorem is the Stone-Čech compactification theorem.

When using the axiom of choice it is not always necessary to apply the most general version, existence of a choice function on any family of nonempty sets. In many proofs, particularly in analysis, it suffices to assume that every *countable* family of nonempty sets has a choice function. Strangely enough, this version of the axiom of choice was more acceptable to the critics of the axiom, although it is as nonconstructive as the general version and it is not clear to me why it should be more plausible.

One consequence of the countable axiom of choice is of course that the union of countably many countable sets is countable (see the proof in

Section 2). This fact is frequently used in real analysis and measure theory; for instance to prove the basic properties of Borel sets and of Lebesgue measure or to show that the ideal of meager sets is closed under countable unions.

The countable axiom of choice is indispensable in descriptive set theory. (Without it, it could happen that the continuum is the union of countably many countable sets.) It is also sufficient for most arguments in descriptive set theory. Still, the favorite of the descriptive set theorists is the following stronger principle (*the principle of dependent choices*):

If ρ is a relation on a nonempty set A such that for every $x \in A$ there exists $y \in A$ with $x \rho y$, then there is a sequence $\{x_m\}_{m=0}^\infty$ of elements of A such that

$$x_0 \rho x_1, x_1 \rho x_2, \dots, x_m \rho x_{m+1}, \dots$$

The principle of dependent choices implies the countable axiom of choice: Given countably many nonempty sets $S_1, S_2, S_3, \dots$, let A consist of all choice functions on the first n sets $S_1, \dots, S_n$ and let $f \rho g$ mean that g extends f . A sequence $f_1, f_2, f_3, \dots$ such that $f_1 \rho f_2$ etc. yields a choice function on $\{S_n\}_{n=1}^\infty$. Moreover, the principle of dependent choices has other useful consequences: for instance, if a linear ordering $<$ is not a well-ordering then there exists an infinite descending sequence $a_0 > a_1 > a_2 > \dots$.

5. Consistency of the axiom of choice

Unlike the question of plausibility, the consistency of the axiom of choice is purely a formal problem of the axiomatic set theory.

A system of axioms Σ for a mathematical theory is *consistent* if there exists no proof of contradiction based on axioms in Σ . As discussed in Chapter D.1, the consistency of a strong enough theory (such as set theory) cannot be established by methods formalizable in that theory. In other words, there can be no formal proof of consistency of axiomatic arithmetic, set theory and similar theories.

However, one can still ask whether a certain axiom A is *consistent relative to* an axiomatic system Σ ; namely whether, assuming that Σ is consistent, it remains consistent upon adding A to it. Another way to say this is that the negation of A is not provable from the axioms of Σ . In the case of the axiom of choice, the question is to show that it is consistent relative to other axioms of set theory, that is that it cannot be refuted by a proof using the other axioms (unless these axioms are themselves inconsistent).

Consistency of the axiom of choice was proved by Gödel in 1939 (along with consistency of the continuum hypothesis). I will outline the main idea of Gödel's proof, but first I would like to say a few words about consistency proofs in general.

The reader is probably familiar with the problem of Euclid's parallel postulate and with the various models of noneuclidean geometries. These models establish unprovability of the parallel postulate in geometry by satisfying all other geometrical axioms except the parallel postulate. In general, in order to show that an axiom is consistent with a theory Σ (that its negation is not provable), one constructs a model of Σ in which the axiom is satisfied.

I shall outline two methods of getting a model of set theory that satisfies the axiom of choice. Both methods are due to Gödel.

The first model consists of *constructible sets*. The idea behind constructible sets is that since the axioms of set theory postulate that various constructions can be performed, there must be a minimal collection of sets closed under all possible set-theoretical constructions. Thus, one constructs the *constructible model* L (the universe of constructible sets) by transfinite induction, starting with the empty set and closing off under set-theoretical operations. (For some more details see Chapter B.5 on constructible sets.) The constructible model satisfies all the axioms of set theory, and also the axiom of choice. The reason why the axiom of choice is true in the model is that one can arrange all the sets in the model into a transfinite sequence: a constructible set X precedes a constructible set Y if it is constructed before Y . In other words, in the model L we have a well-ordering of the universe, and so the axiom of choice holds in L .

The other construction uses *definable sets*. The model consists of all sets that are hereditarily ordinal-definable (HOD). That means sets definable by a formula containing ordinal numbers as parameters, and such that all their elements are so definable, and all elements of their elements etc. The model HOD is closed under set-theoretical operations, and for that reason (more or less) satisfies all axioms of set theory. Again, we have a well-ordering of the universe in HOD: we may enumerate all possible ways of defining a set, and use this enumeration and the natural well-ordering of the ordinal parameters to well-order the HOD sets.

6. Independence of the axiom of choice

In 1963, Cohen constructed a model of set theory in which the axiom of choice is false, thus showing that it cannot be proved from other axioms of

set theory. Cohen introduced a new powerful method of construction of models, the method of *forcing*, and used it to prove independence of the continuum hypothesis, and the axiom of choice.

The method of forcing is explained in Chapter B.4, so let me only recall the main ideas of the method and some basic facts about generic models. One starts with a given model of set theory, called the *ground model*, and tries to extend this model to a larger model that has the same ordinal numbers but has new sets that do not belong to the ground model. Since the work is done inside the ground model, the new sets to be adjoined to the ground model are only hypothetical, or imaginary, and cannot be described completely in the ground model. Instead, one singles out some conditions that one forces upon the new sets. The key concept is the notion of *forcing*, the relation “ p forces σ ” where p is a forcing condition and σ is a sentence involving names of the new sets. Given a sentence σ , some conditions may force it true and some may force it false, but there is always a forcing condition p which *decides* σ , that is either p forces σ or p forces $\neg \sigma$.

To construct a generic model, one postulates existence of a *generic* set of conditions G , a set of forcing conditions that is consistent and for every sentence σ contains a condition that decides σ . A generic set is generally not in the ground model. Using G , every sentence of the forcing language is declared either true or false, and every name is assigned a definite, completely determined set (possibly in the ground model, possibly a new set). The collection of all sets so obtained includes the ground model, contains G and is closed under all set-theoretical constructions. It is a model of set theory and is called a *generic extension* of the ground model. The important property of a generic extension is that it can be described inside the ground model: the main theorem states that a sentence is true in the extension iff it is forced by some condition in G .

If the ground model M satisfies the axiom of choice then the generic extension $M[G]$ also satisfies the axiom of choice. Thus if we want to obtain a model in which the axiom of choice fails we have to do an additional construction. The idea is that the new sets in $M[G]$ are very much alike and so that there is no *definable* well-ordering in $M[G]$. Thus we take an infinite collection $A \in M[G]$ of, say, new sets of integers $A = \{a: a \in A\}$ and consider a model $N = M(\{a: a \in A\})$ obtained by adjoining the sets $a \in A$ to the ground model. We have $M \subset N \subset M[G]$, and since we have not adjoined a well-ordering of A , we expect that there is no well-ordering of A in N .

The construction of N , the *symmetric extension* of M , uses an idea that

goes back to Fraenkel, who already in the 1920's suggested a method to show that the axiom of choice is unprovable. His ideas were worked out by Mostowski in the 1930's who introduced a construction of models known as Fraenkel–Mostowski models, or *permutation models*.

While the Fraenkel–Mostowski method gives models in which the axiom of choice is false, it does not solve the independence problem in set theory, since the underlying universe is not the universe of set theory. The Fraenkel–Mostowski universe (see Fig. 2) differs from the ordinary set theory by assuming existence of *atoms* (or *urelements*), objects that have no elements. The Fraenkel–Mostowski universe consists of all sets built up from the atoms, while the true set-theoretical universe is built up from the empty set. (See the discussion in Chapter B.1.)

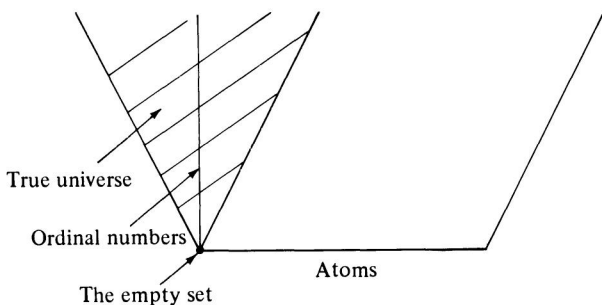


Fig. 2. The Fraenkel–Mostowski universe.

As shown in Fig. 2, the true universe is a part of the Fraenkel–Mostowski universe; I shall call it the *kernel*.

The useful property of the atoms is that they are all alike. This fact is instrumental in the Fraenkel–Mostowski method. I will now describe the simplest example of a permutation model. Let A , the set of all atoms, be infinite. Every permutation π of A can be extended to an automorphism of the FM universe: when X is a set and $\pi(x)$ has been defined for all $x \in X$, we let $\pi(X) = \{\pi(x) : x \in X\}$. Only the sets outside the kernel are moved by π , since $\pi(\emptyset) = \emptyset$ and so $\pi(X) = X$ for every X in the kernel.

Let us call a set X *symmetric*, if there exists a finite set of atoms $\{a_1, \dots, a_n\}$ (a *support* of X) such that whenever π is a permutation of A such that $\pi a_1 = a_1, \dots, \pi a_n = a_n$, then $\pi(X) = X$. Let $\mathcal{U}$ be the class of all hereditarily symmetric sets. The class $\mathcal{U}$ is closed under all operations and it follows that $\mathcal{U}$ is a model of set theory with atoms. Clearly, all sets in the

kernel are symmetric and so $\mathcal{U}$ includes the kernel; $\mathcal{U}$ also includes all atoms since every atom is its own support. It turns out that if a set S of atoms is in $\mathcal{U}$, then either S is finite or $A - S$ is finite: it is easy to see that an infinite set of atoms with an infinite complement has no support!

Now it is clear that the axiom of choice fails in $\mathcal{U}$. The set A cannot be well-ordered, since otherwise it could be divided into two infinite sets.

The Fraenkel–Mostowski method is very simple and has been used to obtain numerous independence results. However, these results do not give any information about the true sets, since the kernel is not affected by the construction of a permutation model. In the example I just gave, there is a set that cannot be well-ordered, but it is a set of atoms, not a set of real numbers or some other genuine mathematical sets.

The ideas of permutation models can be combined with the forcing method and one can thus construct models of true set theory in which the axiom of choice fails. As I mentioned earlier, one constructs a *symmetric* model N such that $M \subset N \subset M[G]$. The idea of permutations is employed as follows: We consider permutations of forcing conditions (or automorphisms of the corresponding Boolean algebra) and use these permutations to construct permutations of *names* (or automorphisms of the Boolean-valued model). Then we extend the ground model M by adding only those new sets that have a *symmetric name* (and so do their elements, and the elements of their elements etc.). In this way we obtain a collection $N \subseteq M[G]$ which includes M because no permutation moves the canonical names for sets in the ground model. N is a model of set theory, a *symmetric extension* of M .

Arguments very similar to those I gave above for a permutation model can be used in this method and one can obtain models without the axiom of choice. For example, the simplest case of a symmetric model is obtained when we use an infinite set A of names of generic sets of integers and use permutations of A and finite supports in a similar way as we did in the FM case. In the resulting model $N = M(\{a : a \in A\})$, the set A is an infinite set of sets of integers and cannot be well-ordered. In fact, no infinite subset of A can be well-ordered and so A is an example of a *Dedekind set*, an infinite set that has no countable subset. Since sets of integers can be identified with real numbers, we have an example of a Dedekind set of real numbers.

The similarity between permutation models and symmetric models can be exploited in a very general fashion and in the next section I shall discuss how the results in set theory with atoms can be uniformly transformed into independence results in set theory.

7. Transfer theorems

As I mentioned in Section 6, the method of symmetric models of set theory uses ideas developed earlier for Fraenkel–Mostowski models. For example the model $M(\{a : a \in A\})$ used by Cohen to prove independence of the axiom of choice is analogous to the simplest permutation model discussed above. Instead of atoms, Cohen's model uses mutually generic sets of integers. However, the analogy between the permutation model and Cohen's model is not complete. We have seen that in the permutation model, the set A cannot be divided into two disjoint infinite sets. On the other hand, in Cohen's model, A is a set of real numbers, and every infinite set of real numbers can be divided into two disjoint infinite sets (in fact every infinite linearly ordered set can). The difference is due to the fact that in Cohen's model, A carries a structure that prevents its elements from being completely alike, as is the case with the atoms.

In another Fraenkel–Mostowski model, the set A is the union of countably many pairs $\{a_n, b_n\}$ of atoms, and has the property that the countable set of pairs $\{\{a_n, b_n\} : n \in N\}$ has no choice function. (Here the atoms are like the socks in Russell's example.) Since every family of finite sets of real number has a choice function, one cannot hope to construct a symmetric model analogous to this FM model, with atoms being replaced by real numbers. Still, another model of Cohen gives exactly such result, but the sets a_n, b_n are *sets of real numbers*. In other words, one gets a better analogy between permutation models and symmetric extensions, if the place of atoms is taken by more abstract, less distinguishable sets. It turns out, that if we let *sets of sets of ordinals* play the role of atoms, we get a quite satisfactory analogy between permutation models and symmetric models. The following theorem shows that any permutation model can be embedded in a symmetric model of set theory “with a prescribed degree of accuracy”.

If S is a set and α an ordinal number let $\mathcal{P}^\alpha(S)$ denote the α -th iteration of the power set operation:

$$\mathcal{P}^1(S) = \mathcal{P}(S) = \{X : X \subseteq S\},$$

$$\mathcal{P}^{\alpha+1}(S) = \mathcal{P}^\alpha(S) \cup \mathcal{P}(\mathcal{P}^\alpha(S)),$$

$$\mathcal{P}^\alpha(S) = \bigcup_{\beta < \alpha} \mathcal{P}_\beta(S) \quad (\text{if } \alpha \text{ is a limit ordinal}).$$

7.1. EMBEDDING THEOREM (Jech–Sochor, see Fig. 3). *Let $\mathcal{U}$ be a permutation model, let A be its set of atoms, and let α be an ordinal number in $\mathcal{U}$.*

There exists a symmetric model N of set theory and an embedding $e : \mathcal{U} \rightarrow N$ such that $\mathcal{P}^\alpha(A)$ in $\mathcal{U}$ is $\in$ -isomorphic to $\mathcal{P}^\alpha(e(A))$ in N .

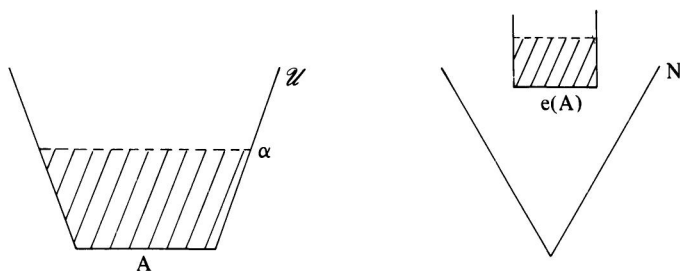


Fig. 3.

The model N is a symmetric extension of the kernel M of the model $\mathcal{U}$ and the set $e(A)$ consists of sets of sets of ordinal numbers of N .

The import of the embedding theorem is that many independence results obtained in the set theory with atoms by Fraenkel–Mostowski method can be automatically transferred into ordinary set theory. There is a large class of statements (which I will not describe here) to which this transfer method is applicable; they are all *existential* statements of a certain kind.

A typical example is the statement “there exists a set that cannot be linearly ordered”. Let $\mathcal{U}$ be a permutation model which has a set that cannot be ordered. For simplicity, let us assume that A itself cannot be ordered. Then we construct a model of set theory in which $\mathcal{U}$ can be embedded so that $\mathcal{P}^\omega(A)$ is isomorphic to $\mathcal{P}^\omega(e(A))$. It follows that $e(A)$ cannot be ordered in N , since any ordering of A , a binary relation on A , would have to be a member of $\mathcal{P}^\omega(A)$.

There are numerous applications of this transfer method, and all statements that are being transferred are existential statements. However, this method does not apply to situations when one wants to prove independence of one statement from another. Consider this example: we want to show that the axiom of choice is stronger than the ordering theorem; we want a model in which the axiom of choice fails but still every set can be linearly ordered. (This is a result of Lévy.)

We construct a permutation model (due to Mostowski) and wish to transfer the independence result from set theory with atoms into set theory. The negation of the axiom of choice transfers easily by the above method; the statement “every set can be ordered” does not. However, it is possible to investigate the structure of the permutation model and impose a similar structure on the corresponding symmetric model. In case of the ordering theorem, it suffices to use the finite supports mentioned in Section

6, and introduce a similar support structure in N . This itself is enough that the statement "every set can be ordered" can be transferred.

The transfer method has been perfected in recent years by D. Pincus, and although some of the transfer theorems seem to be ad hoc formulations of specific applications, they cover most independence results obtained by the Fraenkel–Mostowski method.

Since the presence of atoms makes Fraenkel–Mostowski models different from models of set theory, it is to be expected that not every independence result can be transferred. I shall conclude this section with an example of a statement that is equivalent to the axiom of choice in ordinary set theory but is known to hold in a permutation model in which the axiom of choice fails.

(*The axiom of multiple choice.*) Every family $\mathcal{F}$ of nonempty sets has a function f with the property that $f(X)$ is a nonempty finite set of X , for every $X \in \mathcal{F}$.

8. Mathematics without the axiom of choice

Since the axiom of choice is consistent with other axioms of set theory, there is no reason why it should not be admissible in mathematical proofs. However, since the axiom has a different character than the other axioms, it is useful to investigate models of set theory that do not satisfy the axiom of choice. The situation is analogous to noneuclidean geometries: by studying these models, one learns which theorems have to use the axiom and what are the implications among various consequences and weaker versions of the axiom.

Most interesting among the large number of existing results are those that deal with real numbers. Particularly interesting is the result of Solovay who constructed a model of set theory in which every set of reals is Lebesgue measurable. In Solovay's model, the principle of dependent choices holds, and so all the standard theorems of Lebesgue measure theory and descriptive set theory can be proved. The universe of Solovay's model is thus very appealing to an analyst, since it lacks the unnatural counterexamples like Vitali's nonmeasurable set, a set without the property of Baire, a discontinuous additive function etc.

As I stated earlier, the model constructed by Cohen contains a *Dedekind* set of reals, that is an infinite set that has no countable subset. Existence of such set A provides several interesting examples. To start with, it is easy to show that the set A has a limit point, a . However, the point a cannot be a limit of any sequence in $A - \{a\}$, since A is Dedekind. Which shows that

the two usual definitions of a limit point (the one using neighborhoods and the one using sequences) are not equivalent without the axiom of choice.

Continuity of real-valued functions is also defined in two ways: the ε - δ -definition is one, and the other that says that $\lim x_n = x$ implies $\lim f(x_n) = f(x)$. Using a Dedekind set of reals, one can construct a function which satisfies the limit definition of continuity, but is discontinuous nevertheless.

Another interesting model, due to Feferman and Lévy, has the property that the set of all real numbers is the union of countably many countable sets.

The permutation models, together with the transfer theorems, are also a source of interesting counterexamples. The following examples were constructed by Läuchli in permutation models, and transfer to set theory by the embedding theorem (except the algebraic closure, whose transfer is due to Pincus):

- (a) a vector space that has no basis;
- (b) a vector space that has two bases of different cardinalities;
- (c) a free group whose commutator subgroup is not a free group;
- (d) a field that has no algebraic closure.

In Section 4, I have discussed at length the prime ideal theorem. Since it implies the ordering theorem, and the ordering theorem is not provable in set theory (without choice), it follows that the prime ideal theorem is unprovable. It follows from the axiom of choice, but it is not equivalent to it: Halpern and Lévy showed that the prime ideal theorem does not imply the axiom of choice.

Concerning ultrafilters, Feferman constructed a model in which there is no nonprincipal ultrafilter on the set of all integers; Blass extended his result by showing that in a related model, there is no nonprincipal ultrafilter at all.

The theory of cardinal numbers becomes quite interesting when the axiom of choice is dropped. To start with, without the axiom of choice, one cannot prove that any two cardinals are comparable; it can only be proved that the relation $|X| < |Y|$ is a partial ordering of cardinals. Not much more can be proved about this partial ordering, since by a result of this writer, given any partially ordered set, there exists a model of set theory which has a set of cardinals isomorphic to the given partially ordered set.

There is a number of results concerning *Dedekind cardinals* (cardinals of Dedekind sets). For example, it is possible to have an infinite cardinal m such that 2^m is a Dedekind cardinal. (While it is easy to show that $2^{2^m} \geq \aleph_0$ for any infinite m .)

An old result of Tarski states that if $m \cdot m = m$ for every infinite m , then the axiom of choice holds. A recent construction of Sageev shows that this is not the case with the equation $m + m = m$. It holds in his model but the axiom of choice fails.

All successor alephs $\aleph_{\alpha+1}$ are regular cardinals; that is if the axiom of choice holds. In Feferman–Lévy’s model mentioned above, the cardinal $\aleph_1$ is singular: there exists an increasing sequence $\{\alpha_0, \alpha_1, \dots, \alpha_n, \dots\}$ whose limit is ω_1 . It is an open problem to construct a model of set theory in which *every* limit ordinal number is the limit of a countable sequence. (It is only known that a large cardinal assumption is necessary for this construction.)

I shall end this section with an interesting combinatorial problem that has been a subject of a number of articles and whose solution involves, beside the set-theoretical methods discussed above, some number theory and some finite group theory. For any integer n , let us consider the following statement:

C_n If $\mathcal{F}$ is a family of sets that have exactly n elements, then $\mathcal{F}$ has a choice function.

It was Tarski who inspired the investigation of these statements, and observed that C_2 implies C_4 :

Let A be a four-element set and let us assume that we have a function f that chooses from two-element sets. We shall use f to determine which element of A to choose. (We shall get a well-defined procedure, uniform for all four-element sets.) There are six two-element subsets of A . For each $x \in A$, let $q(x)$ be the number of all pairs $\{x, y\} \in A$ such that $f(\{x, y\}) = x$. Let q be the least such $q(x)$ and let $B = \{x \in A : q(x) = q\}$. It is easy to see that $B \neq A$; thus B has 1, 2 or 3 elements. If B has one element, we choose this element; if B has 3 elements, we choose the element that is not in B . If B has two elements, we choose $f(B)$.

This nice observation raises a number of questions. The general problem is to determine which combinations of C_n ’s imply other combinations of C_n ’s. The various theorems in literature give necessary and sufficient conditions (number or group theoretical) for an implication to be provable. One special case is the theorem that “ C_2 implies C_n ” is provable if and only if $n = 1, 2$ or 4 . The only if part was proved by Mostowski for set theory with atoms and transfers to set theory by the methods of Jech–Sochor and Pincus. The reader might find interesting that Mostowski’s proof makes use of number theory, in particular Bertrand’s postulate

9. Definable choice

In this section, I will consider the question when one can *define* a choice function. In Section 5, I presented two models of set theory, the constructible universe L and the model HOD of hereditarily ordinal-definable sets. In both models, the universe has a definable well-ordering. (The model L is the least model that contains all ordinal numbers; on the other hand, HOD is the largest model that has a definable well-ordering.)

Generic models provide numerous examples on definable choice. There exist both models which have nonconstructible sets and still have a definable well-ordering of the universe and models which satisfy the axiom of choice, but the choice functions are not definable. For instance, in the Cohen's model $M[G]$ from Section 6, the set of all reals does not have a definable well-ordering. In a related model, every definable well-ordering of a set of reals is countable.

The following question belongs rather to descriptive set theory: Let A be a set of real numbers and let $\mathcal{F} = \{S_x : x \in A\}$ be a family of nonempty sets of reals, such that each S_x is defined from x in some uniform way (for instance each S_x is a Π_1^1 set with code x). Can we define a choice function $\{a_x : x \in A\}$ on $\mathcal{F}$?

Questions of this type arise frequently in descriptive set theory (see Chapter B.6). For instance, the *uniformization theorem* of Novikov–Kondo–Addison states that if P is a binary Π_1^1 relation on the reals then there exists a Π_1^1 function f which is a subset of P and has the same projection (see Fig. 4).

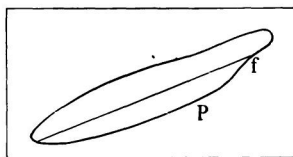


Fig. 4.

The picture explains how the uniformization theorem relates to the above question.

No theorem of that sort can be proved for Π_2^1 sets: The set of all nonconstructible reals is Π_2^1 , and in the Cohen's model mentioned before, no nonconstructible real is definable; this gives an example of a nonempty Π_2^1 set of reals without definable elements.

10. Determinacy — an alternative to the axiom of choice

Since the axiom of choice has several consequences that may not be considered quite desirable (like the existence of nonmeasurable sets), attempts have been made to formulate axioms that contradict the axiom of choice and have more desirable consequences. (Here again, we have the analogy with noneuclidean geometries.) The most interesting alternative to the axiom of choice is the *axiom of determinacy*.

Every set A of infinite sequences of integers defines the following infinite game G_A of two players: Player I plays an integer n_0 , player II responds by playing an integer n_1 , then player I plays n_2 , player II plays n_3 , etc. If the resulting sequence $\{n_0, n_1, n_2, \dots\}$ is in A , player I wins and otherwise player II wins. The game G_A is *determined* if either player I has a winning strategy or player II has a winning strategy. The *axiom of determinacy* states that for every such set A of sequences, G_A is determined.

Using a well-ordering of the set of all sequences of integers, one can construct a game that is not determined. Thus the axiom of determinacy contradicts the axiom of choice.

The axiom of determinacy is particularly appreciated by the descriptive set theorists. For one thing, it implies the countable axiom of choice, and so the basic theorems on real numbers are not affected by the absence of the axiom of choice. It also implies that every set of reals is Lebesgue measurable, has the property of Baire and is either countable or of cardinality $2^{\aleph_0}$. Moreover, the axiom of determinacy settles various problems on projective sets, like uniformization and reduction theorems.

Apart from the desirable consequences that the axiom of determinacy has in descriptive set theory, there is not much to be said in favor of the axiom as an alternative to the axiom of choice. For instance, it implies that $\aleph_1$ and $\aleph_2$ are measurable cardinals, $\aleph_3, \aleph_4, \aleph_5, \dots$ are singular, then $\aleph_{\omega+1}$ and $\aleph_{\omega+2}$ are measurable again. Still, the axiom of determinacy is extremely interesting. Since it implies various large cardinal properties, one has to start with large cardinals if one hopes to prove consistency of the axiom of determinacy. This seems to be a hard problem, and so far, we do not yet know whether the various consequences of determinacy are consistent. For instance, one of the consequences of determinacy is the following statement:

- (*) Every subset of $\aleph_1$ either contains or is disjoint from a closed unbounded set.

This statement implies that $\aleph_1$ is a measurable cardinal. Although this is known to be consistent, the statement (*) appears to be much stronger (although this is at present just a speculation).^{*} It seems that to establish consistency of (*) or of similar statements would be the first step in attacking the problem of consistency of the axiom of determinacy, which is certainly the most interesting open problem that involves the axiom of choice.

References**

FRAENKEL, A.A., Y. BAR-HILLEL and A. LÉVY

[1973] *Foundations of Set Theory* (North-Holland, Amsterdam).

JECH, T.

[1973] *The Axiom of Choice* (North-Holland, Amsterdam).

^{*} *Added in proof.* Martin and Mitchell confirmed this speculation by showing that (*) implies existence of models of set theory with many measurable cardinals.

^{**} The reader who would like references to the original papers, containing the theorems discussed in the article, is advised to consult the comprehensive bibliography of either FRAENKEL, BAR-HILLEL and LÉVY [1973] or JECH [1973].

Combinatorics

KENNETH KUNEN

Contents

Introduction	372
1. Notation	372
2. C.u.b. and stationary sets	372
3. Enumeration principles	375
4. Trees	381
5. Almost disjoint sets	387
6. Partition calculus	390
7. Large cardinals	396
Appendix: Ridiculously large cardinals	399
References	400

Introduction

We consider this chapter to be a short text, rather than a survey — i.e., many of the stated theorems are actually proved. Our intent is to introduce the reader to the basic methods of combinatorial set theory.

We assume familiarity with naive set theory, as in HALMOS [1960] or Chapter B.1. A knowledge of logic is neither necessary, nor even desirable.

Except for an occasional trivial remark, none of the results in this paper are due to the author. We have made no attempt to attach names to each theorem or to refer to original sources; references are intended only to indicate areas for further reading. Some concepts have become so intimately connected with a name (e.g., Laplace transform) that it would be impossible to mention them without their founder, but others of far greater importance have become part of the folklore of the subject. Those who feel that their name has been left out may take solace from the fact that we do not invoke Newton or Leibniz each time we use a derivative.

1. Notation

We review here some terminology. Greek letters are used for (von Neumann) ordinals. $\text{cf}(\alpha)$ is the cofinality of α , the least ordinal β such that there is an order preserving mapping $f: \beta \rightarrow \alpha$ whose range is cofinal in α . Cardinals are initial ordinals; ω_α is the α -th infinite cardinal. λ^+ is the least cardinal greater than λ . $|X|$ is the cardinality of the set X . A cardinal κ is *regular* if $\text{cf}(\kappa) = \kappa$; otherwise κ is *singular*.

$\mathcal{P}(X)$ is the set of subsets of X and X^Y is the set of functions from Y to X . $X^{<\alpha} = \bigcup \{X^\xi : \xi < \alpha\}$. $f \upharpoonright X$ is the restriction of the function f to the set X .

If κ and λ are cardinals, we perpetuate the standard confusing convention of using κ^λ also for $| \kappa^\lambda |$ and $\kappa^{<\lambda}$ for $| \kappa^{<\lambda} |$. So when λ is infinite, $\kappa^{<\lambda} = \sup \{ \kappa^\theta : \theta < \lambda \text{ \& } \theta \text{ is a cardinal} \}$. $\exp(\kappa)$ is used for 2^κ when the typesetting demands it, as in $\exp(\exp(\exp(\omega_2)))$.

$\mathbb{R}$ is the set of real numbers; $\mathbb{Q}$ is the set of rational numbers. $c = |\mathbb{R}| = |\mathcal{P}(\omega)| = 2^\omega$.

2. C.u.b. and stationary sets

The feature that distinguishes the subject of this paper from the

elementary set theory in high school mathematics is the use of transfinite induction on infinite ordinals.

The purpose of this section is partly to develop your intuition about ordinals and partly to introduce some concepts which will be useful later on. In many ways, we may think of the ordinals as an extension of the natural numbers, but a new phenomenon which appears only at the uncountable is that of c.u.b. and stationary sets.

Some definitions. Fix κ a regular uncountable cardinal. If $C \subseteq \kappa$, we call C *closed* iff whenever $\gamma < \kappa$ and $C \cap \gamma$ is unbounded in γ , $\gamma \in C$ (equivalently, C is closed in the order topology). C is *c.u.b.* iff C is closed and unbounded in κ .

Examples of c.u.b. sets are the set of limit ordinals $< \kappa$ and the set of limits of limits. $\{\gamma < \kappa : \gamma \text{ is a cardinal}\}$ is always closed in κ ; it is unbounded iff κ is a limit cardinal (and hence weakly inaccessible, since κ is regular).

There is an analogy here with measure theory. One should think of c.u.b. sets as being large, or almost everything, or of probability measure 1. Then the intersection of two large sets should be large. In fact,

2.1. LEMMA. *The intersection of $< \kappa$ c.u.b. subsets of κ is c.u.b.*

PROOF. Let C_ξ be c.u.b. for $\xi < \alpha$, where $\alpha < \kappa$. It is easy to see that $\bigcap_\xi C_\xi$ is closed. To see that it is unbounded, define $f_\xi : \kappa \rightarrow \kappa$ so that $f_\xi(\gamma)$ is the least ordinal in C_ξ larger than γ . Let $g(\gamma) = \sup\{f_\xi(\gamma) : \xi < \alpha\}$. $g(\gamma) < \kappa$ since κ is regular. Define $h(\gamma, n)$ inductively by $h(\gamma, 0) = \gamma$; $h(\gamma, n+1) = g(h(\gamma, n))$. Let $\gamma^* = \sup_n h(\gamma, n)$. Then $\gamma < \gamma^* < \kappa$, and for each ξ , $C_\xi \cap \gamma^*$ is unbounded in γ^* , so $\gamma^* \in \bigcap_\xi C_\xi$. $\square$

The reader should note why the above would be nonsense if κ were allowed to equal ω .

To continue our analogy with measure theory, stationary sets are those which are not of measure 0 — i.e., we call $S \subseteq \kappa$ *stationary* iff for all c.u.b. $C \subseteq \kappa$, $S \cap C \neq \emptyset$. Then A is non-stationary (i.e. of measure 0) iff $A \cap C = \emptyset$ for some c.u.b. set C .

2.2. LEMMA. (a) *The union of $< \kappa$ non-stationary sets is non-stationary.*

(b) *If S is stationary and C is c.u.b., then $C \cap S$ is stationary.*

(c) *If $\alpha < \kappa$, S is stationary, and $f : S \rightarrow \alpha$, then $f^{-1}\{\xi\}$ is stationary for some $\xi < \alpha$.*

The lemma is easily checked using 2.1. Intuitively, (a) says that a union of a small number of small sets is small, (b) that the intersection of a set of measure 1 with a set of positive measure has positive measure, and (c) that a set of positive measure cannot be partitioned into a small number of sets of measure 0.

The analogy with measure theory can only be carried so far. For example, we shall see in Section 3 that there is a family of κ disjoint stationary subsets of κ . Note that it is not obvious at this point that one can even get 2.

The following generalization of 2.2c, known as the pressing-down lemma, is fundamental in many combinatorial arguments.

2.3. THEOREM (Fodor). *Suppose $S \subseteq \kappa$ is stationary, $f: S \rightarrow \kappa$, and $\forall \eta \in S (f(\eta) < \eta)$. Then for some ξ , $f^{-1}\{\xi\}$ is stationary.*

A special case of 2.3 is that there can be no 1-1 function $f: \{\eta: 0 < \eta < \kappa\} \rightarrow \kappa$ such that $\forall \eta (f(\eta) < \eta)$. This seems counterintuitive if you think of the function $n - 1$ on the natural numbers — but remember, $\kappa > \omega$.

PROOF OF THEOREM 2.3. Assume there is no such ξ . Then for each ξ , there is a c.u.b. C_ξ such that $\forall \eta \in C_\xi \cap S (f(\eta) \neq \xi)$. Let $D = \{\eta: \forall \xi < \eta (\eta \in C_\xi)\}$. Then $D \cap S = \emptyset$, so we shall obtain a contradiction if we show that D is c.u.b. As usual, that D is closed is easy. To see that D is unbounded, fix $\gamma < \kappa$. Let $\gamma_0 = \gamma$; let γ_{n+1} be some ordinal $> \gamma_n$ in $\bigcap \{C_\xi: \xi < \gamma_n\}$ (which is c.u.b. by 2.1). Then $\sup_n \gamma_n \in D$. $\square$

We conclude with a version of the Löwenheim–Skolem theorem (see Chapter A.2). It is well-known that every group has a countable subgroup. We shall show that if $\cdot: \omega_1 \times \omega_1 \rightarrow \omega_1$ is a group operation, then $\{\alpha < \omega_1: (\alpha, \cdot)$ is a subgroup of $(\omega_1, \cdot)\}$ is c.u.b. More generally, a finitary function on κ is a function from $\kappa^k \rightarrow \kappa$ for some $k \in \omega$. Then:

2.4. THEOREM. *If $\kappa > \omega$ is regular and $f_n (n \in \omega)$ are finitary functions on κ , then $C = \{\alpha < \kappa: \forall n (\alpha \text{ is closed under } f_n)\}$ is c.u.b.*

PROOF. C is clearly closed. To see that it is unbounded, fix $\gamma < \kappa$. Say $f_n: \kappa^{k_n} \rightarrow \kappa$. Let $\gamma_0 = \gamma$; let γ_{m+1} be the maximum of γ_m and $\sup\{f_n(s): n \in \omega \text{ and } s \in (\gamma_m)^{k_n}\}$. Then $\sup_m \gamma_m \geq \gamma$ and is in C . $\square$

Although we have avoided explicit use of model-theoretic notions in 2.4,

the reader of Chapter A.2 will see that it shows the following: If $\mathfrak{A}$ is a structure for a countable language and $\mathfrak{A}$ has base set κ , then $\{\alpha < \kappa : \mathfrak{A} \upharpoonright \alpha < \mathfrak{A}\}$ is c.u.b. in κ .

3. Enumeration principles

Under this heading we shall group three related principles of combinatorial set theory.

The first enumeration principle we discuss is the axiom of choice (AC). AC is not provable from the other axioms of set theory (see Chapter B.2). Stated in the form that the cartesian product of non-empty sets is non-empty, AC seems intuitively obvious, but stated in the form that every set can be well-ordered, AC begins to look suspicious, since there is no “natural” way to well-order the real numbers. Nevertheless, in keeping with traditional mathematical practice, we shall continue to use AC (as we did in Section 2) without further comment.

AC has a number of consequences in analysis that seem somewhat pathological. A simple example is:

3.1. THEOREM. *There is a function $f : [0, 1] \rightarrow [0, 1]$ whose graph has outer Lebesgue measure 1 in the square.*

Of course, the graph of any reasonable function has measure 0, but an f satisfying 3.1 may easily be constructed by transfinite induction. Let K_α ($\alpha < c$) enumerate all closed subsets of $[0, 1] \times [0, 1]$ of positive measure. By induction on $\beta < c$, pick p_β, q_β so that:

(1) $\alpha < \beta \rightarrow p_\alpha \neq p_\beta$, and

(2) $\langle p_\beta, q_\beta \rangle \in K_\beta$.

Note that the choice of such p_β, q_β is possible, since by Fubini's theorem $\{p : \exists q \langle p, q \rangle \in K_\beta\}$ has positive measure and hence cardinality c . Take f so that $f(p_\beta) = q_\beta$ for all β . Then the complement of the graph of f contains no closed subsets of positive measure, and hence has inner measure 0.

A deeper application of AC is the Banach–Tarski paradox (BANACH and TARSKI [1924]), which says that the Earth may be decomposed into finitely many pieces and reassembled to form a sphere with the size of the Sun. To see this, apply Theorem 3.3 of Chapter B.2, plus the remarks on $\approx$ there.

A use of AC more relevant to this paper is:

3.2. THEOREM (ULAM [1930]). *If $S \subseteq \omega_1$ is stationary, S may be decomposed into ω_1 disjoint stationary subsets.*

PROOF. By AC, pick, for each $\alpha < \omega_1$, a map f_α from ω onto α . From $n \in \omega$ and $\xi \in \omega_1$, let $A_\xi^n = S \cap \{\alpha : f_\alpha(n) = \xi\}$. For each fixed n , the $A_\xi^n (\xi < \omega_1)$ are disjoint. They may not all be stationary, but it is sufficient to check:

3.3. LEMMA. *For some n , ω_1 of the A_ξ^n are stationary.*

Given the lemma, $\{A_\xi^n : A_\xi^n \text{ is stationary}\}$ satisfies Theorem 3.2. To prove the lemma, note that for each ξ , $\bigcup_n A_\xi^n = \{\alpha : \alpha > \xi\}$ is stationary, so (by 2.2a), there is an n_ξ such that $A_{n_\xi}^\xi$ is stationary. Now take n so that $|\{\xi : n_\xi = n\}| = \omega_1$. $\square$

The $\omega \times \omega_1$ matrix of sets A_ξ^n is known as an *Ulam matrix*.

Theorem 3.2 remains true if ω_1 is replaced by any other regular $\kappa > \omega$. If κ is a successor, the proof is almost verbatim the same. If κ is weakly inaccessible, then 3.2 for $S = \kappa$ is trivial, since the sets $\{\alpha : \text{cf}(\alpha) = \lambda\}$, for λ regular and $\lambda < \kappa$, form the desired partition. However, by Theorem 9 of SOLOVAY [1971], 3.2 holds for any S .

Our second enumeration principle is the continuum hypothesis, CH. If CH is stated by saying that there are no sets of reals of cardinality between ω and c , it is almost believable (try to think of one); but if we use the equivalent version that there is a well-ordering of the real numbers such that every element has only countably many predecessors, it begins to look even more improbable than AC. So we shall not, in this paper, assume CH, and we always state it explicitly as an hypothesis when it is used. CH is consistent with and independent from the usual axioms of set theory, as shown in Chapters B.4 and B.5.

There are a large number of applications of CH to the real numbers (see, e.g., SIERPIŃSKI [1934]). Broadly speaking, the results fall into two classes. The first are really just combinatorial facts always true about ω_1 , which under CH, apply to the reals. The second are intrinsically theorems about the reals, no shadow of which need remain if CH fails.

An example of the first class is the following:

3.4. THEOREM (CH). *There is a countable family of functions $f_n : [0, 1] \rightarrow [0, 1]$ such that $[0, 1] \times [0, 1] = (\bigcup_n f_n) \cup (\bigcup_n f_n^{-1})$.*

This should be compared with 3.1; here we identify a function with its graph. To prove 3.4, it is sufficient to prove the same result with ω_1 replacing $[0, 1]$, in which case CH is not needed. Let, for $\alpha < \omega_1$, g_α map ω onto $\alpha + 1$. Let $f_n(\alpha) = g_\alpha(n)$.

An example of the second class is the existence of a *Luzin set*. A subset $L \subseteq \mathbb{R}$ is called a *Luzin set* iff L is uncountable but $L \cap K$ is countable whenever K is closed and nowhere dense (c.n.w.d.). Such an L has a number of peculiar properties. With regard to category, it is not very small, since no uncountable subset of L is of first category. However, with regard to measure, L is as small as one can get; L has measure 0 under Lebesgue measure or any other non-atomic Borel measure (since for all $\varepsilon > 0$, there is a c.n.w.d. K such that $\mathbb{R} - K$ has measure $< \varepsilon$).

That Luzin sets exist is not provable without some extra set-theoretic axiom. For example, Martin's axiom (see Chapter B.6) plus not CH implies there are no Luzin sets. But:

3.5. THEOREM (LUZIN [1914]). *CH implies there is a Luzin set.*

PROOF. Let K_α ($\alpha < \omega_1$) enumerate the $c = \omega_1$ c.n.w.d. sets. Inductively, pick p_β so that

- (1) $\alpha < \beta \rightarrow p_\beta \neq p_\alpha$, and
- (2) $p_\beta \notin \bigcup_{\alpha < \beta} K_\alpha$.

The construction is possible at stage β by the Baire category theorem, which states that $\mathbb{R}$ is not the union of ω c.n.w.d. sets; in particular,

$$\mathbb{R} - \left[\bigcup_{\alpha < \beta} K_\alpha \cup \bigcup_{\alpha < \beta} \{p_\alpha\} \right] \neq \emptyset.$$

Now, $\{p_\beta : \beta < \omega_1\}$ is a Luzin set. $\square$

One may formulate the basic properties of a Luzin set as intrinsic properties of the set itself. Thus,

3.6. THEOREM (CH). *There is an ordering $(L, <)$, such that*

- (a) *$<$ is a dense total order without endpoints.*
- (b) *In L , every c.n.w.d. (in the order topology) set is countable.*
- (c) *L is uncountable.*

PROOF. Following the notation of the proof of 3.5, let $L = \{p_\beta : \beta < \omega_1\} \cup \mathbb{Q}$. Then (a) and (c) are immediate, and (b) holds because if K is c.n.w.d. in L , the closure of K in $\mathbb{R}$ is c.n.w.d. in $\mathbb{R}$. $\square$

Most statements about analysis which are provable from CH are independent of the negation of CH. This is the case for 3.5 and 3.6. One

that is in fact equivalent to CH is given by the following, which we state without proof.

3.7. THEOREM (Erdős). *CH is equivalent to the statement: There is an uncountable family $\mathcal{F}$ of entire functions such that for each complex number z , $\{f(z): f \in \mathcal{F}\}$ is countable.*

Our next enumeration principle is Jensen's $\diamond$. $\diamond$ asserts: there is a sequence $\langle A_\alpha: \alpha < \omega_1 \rangle$ such that each $A_\alpha \subseteq \alpha$ and

$$(*) \quad \forall A \subseteq \omega_1 [\{\alpha: A \cap \alpha = A_\alpha\} \text{ is stationary}].$$

$\diamond$ implies CH, since $(*)$ yields $\forall A \subseteq \omega \exists \alpha [A \cap \alpha = A_\alpha]$, but CH does not imply $\diamond$ (Jensen — see DEVLIN and JOHNSBRÅTEN [1974]). However, $\diamond$ does follow from Gödel's axiom of constructibility (see Theorem 11.2 of Chapter B.5). $\diamond$ may also be proved consistent by forcing (see Exercise 4.18 of Chapter B.4).

Like CH, $\diamond$ gives an enumeration of countable sets, but now the enumeration approximates all subsets of ω_1 . Arguments using $\diamond$ resemble CH arguments, but yield stronger results. This can be illustrated by the construction of a Suslin line.

Suslin's hypothesis (SH) is the assertion that any ordering $(L, <)$ satisfying

- (i) $<$ is a dense total order without endpoints,
- (ii) L has the countable chain condition (c.c.c.), i.e., in L there is no uncountable family of disjoint open intervals, and
- (iii) $(L, <)$ is Dedekind complete,

is isomorphic to the real line, $(\mathbb{R}, <)$. SH is consistent with set theory; for example, it follows from Martin's axiom plus not CH (see Chapter B.6), and in fact is consistent with CH (Jensen — see DEVLIN and JOHNSBRÅTEN [1974]). However, $\diamond$ implies not SH; thus, assuming $\diamond$, we shall construct an ordering $(L, <)$ satisfying (i)–(iii) which is not isomorphic to $(\mathbb{R}, <)$; such an ordering is called a *Suslin line*.

In analogy with 3.6, we shall show:

3.8. THEOREM ($\diamond$). *There is an ordering $(L, <)$ such that*

- (a) *$<$ is a dense total order without endpoints.*
- (b) *In L , every c.n.w.d. set is countable.*
- (c⁺) *L is not separable.*

(c⁺) means that no countable subset of L is dense in L . Before we prove

3.8, we point out why it gives us a Suslin line. Let $(L, <)$ satisfy 3.8. Then L satisfies condition (ii), for, if $\{(a_i, b_i): i \in I\}$ were an uncountable family of disjoint open intervals, we could first assume it is maximal (by Zorn's lemma), and then set $K = L - \bigcup_i (a_i, b_i)$; K would be c.n.w.d., but would contain all the a_i and b_i , violating (b). L will not be Dedekind complete, so let L^* be its Dedekind completion; it is easy to see that this preserves the c.c.c. (but not (b)). Then L^* satisfies (i)–(iii), but cannot be isomorphic to $\mathbb{R}$, since this would make L isomorphic to a subspace of $\mathbb{R}$, and hence separable.

As in the case of a Luzin set, we construct the L of 3.8 by induction, eventually avoiding all c.n.w.d. sets. But since L cannot be a subspace of $\mathbb{R}$, there is no natural ordering given in advance from which to pick points. Rather, we must inductively define the order on the points of L as we go along. What the points of L actually are is now irrelevant; to simplify notation, we might as well take L to be ω_1 as a set; thus, we shall construct an order, $\triangleleft$, on ω_1 , to satisfy 3.8.

We define $\triangleleft$ in steps of ω . In the following discussion α and β will range over countable limit ordinals. By induction on α we define an order $\triangleleft_\alpha$ on α so that:

(i) Each $\triangleleft_\alpha$ is a dense total order without endpoints, and

(ii) if $\alpha < \beta$, $\triangleleft_\alpha = \triangleleft_\beta \cap (\alpha \times \alpha)$.

(ii) just says that the orderings extend each other. (i) implies that each $(\alpha, \triangleleft_\alpha)$ is isomorphic to the rationals, $\mathbb{Q}$, but the important thing is the way the orderings are nested. We may take $\triangleleft_\omega$ to be any ordering of ω isomorphic to $\mathbb{Q}$. If β is a limit of limits, (ii) forces us to take $\triangleleft_\beta = \bigcup_{\alpha < \beta} \triangleleft_\alpha$. Likewise, we let $\triangleleft = \bigcup_{\alpha < \omega_1} \triangleleft_\alpha$; then $(\omega_1, \triangleleft)$ satisfies (a) of 3.8. The only thing left to specify in the construction is how to define $\triangleleft_{\beta+\omega}$ from $\triangleleft_\beta$; we must do this in such a way as to make (b) and (c⁺) hold.

(c⁺) is easy. It is sufficient to guarantee that no β is dense in ω_1 (in the order $\triangleleft$). Given $\triangleleft_\beta$, we let D_β be a proper Dedekind cut in $(\beta, \triangleleft_\beta)$ (i.e., D_β is a proper initial segment of β with no supremum). Form $\triangleleft_{\beta+\omega}$ by inserting a copy of $\mathbb{Q}$ into D_β ; i.e., the ordinals $\beta + n$ ($n \in \omega$) are ordered isomorphically to $\mathbb{Q}$, and placed after the elements of D_β and before the elements of $\beta - D_\beta$. Then β will not be dense in $\beta + \omega$, so certainly not in ω_1 either.

We now show how, by judicious choice of the D_β , we may make $(\omega_1, \triangleleft)$ satisfy (b). The idea is to apply the Baire theorem to avoid all previously listed c.n.w.d. sets, but we must first see what the Baire theorem says for countable orderings, like $\mathbb{Q}$. If K is c.n.w.d. in $\mathbb{Q}$ and D is a proper Dedekind cut in $\mathbb{Q}$, we say D avoids K iff there are $a < b$ in $\mathbb{Q}$ with

$[a, b] \cap K = 0$ and $a < D < b$ (i.e. $a \in D$, $b \notin D$). Then the Baire theorem says:

3.9. LEMMA. *If K_n ($n \in \omega$) are c.n.w.d. in $\mathbb{Q}$, there is a proper Dedekind cut D which avoids each K_n .*

PROOF. The closures of each K_n in $\mathbb{R}$ are c.n.w.d., so there is an irrational x which is not in the closure of any K_n . Let D be the cut defined by x . $\square$

Now, let $\langle A_\alpha : \alpha < \omega_1 \rangle$ be given by $\diamond$ to satisfy (*). Applying the lemma, take each D_β so that it avoids all the A_α for $\alpha \leq \beta$ such that A_α is c.n.w.d. in $(\beta, \triangleleft_\beta)$. This completes the description of the construction; we need only check that it works — i.e., that (b) holds.

Let $K \subseteq \omega_1$ be c.n.w.d. in $(\omega_1, \triangleleft)$. $K \cap \alpha$ need not be c.n.w.d. in $(\alpha, \triangleleft)$ for all α , but it is for lots of them. To see this, let $f, g : \omega_1 \rightarrow \omega_1$ and $h, h' : \omega_1^2 \rightarrow \omega_1$ be such that for each $\xi \in \omega_1 - K$, $f(\xi) \triangleleft \xi \triangleleft g(\xi)$ and $(f(\xi), g(\xi)) \cap K = 0$, and for each $\xi \triangleleft \eta$, $h(\xi, \eta), h'(\xi, \eta) \in (\xi, \eta)$, $h(\xi, \eta) \notin K$, and $h'(\xi, \eta) \in K$ whenever $K \cap (\xi, \eta) \neq 0$. Applying Theorem 2.4, $C = \{\alpha < \omega_1 : \alpha \text{ is a limit and } \alpha \text{ is closed under } f, g, h, h'\}$ is c.u.b. If $\alpha \in C$, then closure under f, g , implies that $K \cap \alpha$ is closed in $(\alpha, \triangleleft_\alpha)$, and closure under h implies that it is n.w.d.

By (*), fix $\alpha \in C$ such that $K \cap \alpha = A_\alpha$. We shall be done if we can show that $K \subseteq \alpha$. This follows by (i) of:

3.10. LEMMA. *For all limits $\beta \geq \alpha$,*

- (i) $K \cap \beta = K \cap \alpha$, and
- (ii) *if $\gamma \in \beta - K$, there are $\xi, \eta \in \alpha$ with $\xi \triangleleft \gamma \triangleleft \eta$ and $(\xi, \eta) \cap K = 0$ in $(\omega_1, \triangleleft)$.*

PROOF. Induction on β . For $\beta = \alpha$, use closure under f and g . The induction is trivial at limits, so assume 3.10 holds for β ; we check it for $\beta + \omega$. Now by 3.10 for β , $A_\alpha = K \cap \beta$ is c.n.w.d. in $(\beta, \triangleleft_\beta)$, so D_β avoids A_α . Thus, there are $\gamma \triangleleft \gamma'$ in β such that $[\gamma, \gamma'] \cap K \cap \beta = 0$ and all the ordinals $\beta + n$ ($n \in \omega$) lie in (γ, γ') . Let $\xi, \eta, \xi', \eta' < \alpha$ arise from applying 3.10(ii) to γ, γ' respectively. Then $(\xi, \eta') \cap K \cap \alpha = 0$, whence, by closure of α under h' , $(\xi, \eta') \cap K = 0$. Since all the $\beta + n$ lie in (ξ, η') , (i) and (ii) for $\beta + \omega$ follow immediately. $\square$

This completes our discussion of AC, CH, and $\diamond$. For a more thorough discussion of combinatorial properties generalizing $\diamond$, see Chapter B.5 or DEVLIN and JOHNSBRÄTEN [1974].

4. Trees

Induction along a tree is a generalization of induction on an ordinal and is often useful in combinatorial arguments. The theorems proved in this section with trees will be fairly elementary. Deeper results will be obtained in Section 6.

Some definitions. A *tree* is a partial ordering, $(T, <)$, such that for each $y \in T$, $\{x: x < y\}$ is well-ordered by $<$. The α -th level of T is $\{y: \{x: x < y\} \text{ has type } \alpha\}$. The *height* of T is the first α such that the α -th level of T is empty; then all higher levels are also empty and all lower levels are non-empty.

T' is a *subtree* of T iff T' is obtained by pruning off some branches of T ; i.e. $T' \subseteq T$ and $\forall y \in T' \forall x \in T [x < y \rightarrow x \in T']$.

For each α and set A , the *complete A -ary tree* of height α , $A^{<\alpha}$, is $\bigcup \{A^\xi: \xi < \alpha\}$ (i.e., the tree of $<\alpha$ -sequences from A); in $A^{<\alpha}$, $s \leq t$ iff $s \subseteq t$. When talking about such trees, we use $s^{\frown} a$ ($s \in A^\xi$, $a \in A$) to denote the $t \in A^{\xi+1}$ such that $t \restriction \xi = s$ and $t(\xi) = a$; $\langle \rangle$ denotes the empty sequences and $\text{lh } s = \text{dom}(s)$ (the length of s); formally, $\langle \rangle = 0$ and $s^{\frown} a = s \cup \{\langle \text{lh } s, a \rangle\}$.

The tree T pictured in Fig. 1 is a subtree of the complete binary (2-ary) tree of height 3; T has height 3 — i.e., 3 non-0 levels; its 0-th, 1-th, and 2-th levels are $\{\langle \rangle\}$, $\{\langle 0 \rangle, \langle 1 \rangle\}$, $\{\langle 1, 0 \rangle, \langle 1, 1 \rangle\}$ respectively. Note that our mathematical tree is what is left of a real tree when one removes the leaves, roots, trunk, and branches.

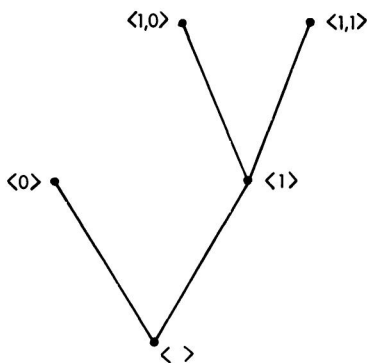


Fig. 1.

The ordinal α is a trivial example of a tree of height α ; its ξ -th level is $\{\xi\}$.

An example of a simple result proved using induction on $2^{<\omega}$ is

4.1. THEOREM. *If X is a closed subset of $[0, 1]$ and has no isolated points, then $|X| = c$.*

An X satisfying the hypothesis of 4.1 is called *perfect*. For the proof, first note:

4.2. LEMMA. *If X is perfect, there are disjoint $X_0, X_1 \subseteq X$ such that X_0 and X_1 are perfect.*

PROOF OF THEOREM 4.1. Define perfect X_s ($s \in 2^{<\omega}$) as follows: $X_{\langle \rangle} = X$; given X_s , let $X_{s \wedge 0}, X_{s \wedge 1}$ be disjoint perfect subsets of X_s . If $f \in 2^\omega$, let $X_f = \bigcap_n X_{f \upharpoonright n}$. Then as f ranges over 2^ω , the X_f are non-empty (by compactness) and disjoint, so $|X| \geq c$. Since $X \subseteq [0, 1]$, $|X| = c$. $\square$

An obvious generalization of 4.1, with the same proof, is that if X is any compact Hausdorff space with no isolated points, then $|X| \geq c$. An analogous result using induction on $2^{<\omega_1}$ is:

4.3. THEOREM (Čech–Pospíšil). *If X is compact Hausdorff and no point of X is a G_δ , then $|X| \geq 2^{\omega_1}$.*

Let us call such an X *pluperfect*. Pluperfect spaces do not arise frequently in applied mathematics. Standard examples are $\beta N - N$, the unit ball of the dual spaces of $L^\infty(\mathbb{R})$ in the weak* topology, and any product of uncountably many compact Hausdorff spaces with more than two points. Before proving 4.3, we prove three easy lemmas about pluperfect X .

4.4. LEMMA. *If $Y \subseteq X$ is a closed G_δ in X , then Y is pluperfect.*

PROOF. If a point of Y were a G_δ in Y , it would be a G_δ in X . $\square$

4.5. LEMMA. *If $U \subseteq X$ is non-empty and open, there is a non-empty closed G_δ $Y \subseteq U$.*

PROOF. Fix $p \in U$. Define inductively open V_n containing p such that $U \supseteq \bar{V}_0 \supseteq V_0 \supseteq \bar{V}_1 \supseteq V_1 \supseteq \bar{V}_2 \supseteq \cdots$. Let $Y = \bigcap_n V_n = \bigcap_n \bar{V}_n$. $\square$

4.6. LEMMA. *There are disjoint non-empty $X_0, X_1 \subseteq X$, each of which is closed G_δ .*

PROOF. Take two disjoint open sets and apply 4.5. $\square$

PROOF OF THEOREM 4.3. Define closed non-0 G_δ 's X_s ($s \in 2^{<\omega_1}$) as follows: $X_{\langle \rangle} = X$; given X_s , let $X_{s \wedge 0}$, $X_{s \wedge 1}$ be disjoint closed G_δ 's which are subsets of X_s ; if $\text{lh } s$ is a limit, $X_s = \bigcap \{X_{s \upharpoonright \alpha} : \alpha < \text{lh } s\}$. If $f \in 2^{\omega_1}$, let $X_f = \bigcap_{\alpha < \omega_1} X_{f \upharpoonright \alpha}$. Then the X_f ($f \in 2^{\omega_1}$) are disjoint and non-empty, so $|X| \geq 2^{\omega_1}$. $\square$

The proof of 4.3 easily generalizes to show that if X is compact Hausdorff and every point in X has character $\geq \kappa$, then $|X| \geq 2^\kappa$. For more on applications of trees to topology, see JUHÁSZ [1971] and Chapter B.7.

We now discuss some questions regarding paths through trees. We call P a *path through* T iff P is totally ordered by $<$ and contains exactly one element from each non-0 level of T . If T has height α and is a subtree $A^{<\alpha}$, we identify a path P with the $f : \alpha \rightarrow A$ such that $P = \{f \upharpoonright \xi : \xi < \alpha\}$. Trees of the form $A^{<\alpha}$ and all trees of successor height trivially have paths, but some trees have none. For example, fix $\gamma \geq \omega$ and let $T = \{s \in \gamma^{<\omega} : s(0) > s(1) > s(2) > \dots\}$. Then T has height ω but no paths, since there are no decreasing ω -sequences of ordinals. For trees of height ω we do have

4.7. LEMMA (König). *If T has height ω and every level of T is finite, then there is a path through T .*

PROOF. Pick x_0 in level 0 of T such that $\{y \in T : y > x_0\}$ is infinite; this is possible since T is infinite and level 0 is finite. Now inductively pick x_n ($n \in \omega$) in level n of T so that for each n , $x_{n+1} > x_n$ and $\{y \in T : y > x_{n+1}\}$ is infinite. Then $\{x_n : n \in \omega\}$ is a path through T . $\square$

The obvious generalization of König's lemma to ω_1 is false:

4.8. THEOREM. *There is a tree T of height ω_1 such that every level of T is countable but there are no paths through T .*

PROOF. Let $S = \{s \in \omega^{<\omega_1} : s \text{ is 1-1}\}$. S is a subtree of $\omega^{<\omega_1}$. There are no paths through S since there are no 1-1 functions from ω_1 to ω . Of course, the levels of S are uncountable, so we shall use a suitable subtree of S . If $s, t \in \omega^\alpha$, say $s \approx t$ iff $\{\xi : s(\xi) \neq t(\xi)\}$ is finite. $\square$

4.9. LEMMA. *There is a sequence s_α ($\alpha < \omega_1$) from S such that whenever $\alpha < \beta$, $s_\alpha \approx s_\beta \upharpoonright \alpha$.*

Assuming 4.9, $T = \bigcup_{\alpha < \omega_1} \{s \in \omega^\alpha : s \in S \text{ and } s \approx s_\alpha\}$ satisfies 4.8. To prove 4.9, define s_α by induction, making sure that $\omega - (\text{range}(s_\alpha))$ is infinite. Then $s_{\alpha+1}$ can be any 1-1 extension of s_α . If γ is a limit and s_α ($\alpha < \gamma$) are given, let $\gamma_n \nearrow \gamma$ ($n \in \omega$). By induction on n , find $s'_{\gamma_n} \in S$ such that $s'_{\gamma_n} \approx s_{\gamma_n}$ and $m < n \rightarrow s'_{\gamma_m} = s'_{\gamma_n} \upharpoonright \gamma_m$. Let $t = \bigcup_n s'_{\gamma_n}$. Let $s_\gamma \in S$ be such that $s_\gamma(\xi) = t(\xi)$ for $\xi \notin \{\gamma_n : n \in \omega\}$ and $\omega - \text{range}(s_\gamma)$ is infinite. $\square$

For any regular κ , we call a κ -Aronszajn tree a tree T of height κ such that all levels of T have cardinality less than κ and T has no paths. Then König's lemma says that there are no ω -Aronszajn trees, whereas 4.8 shows that there is an ω_1 -Aronszajn tree. The argument of 4.8 easily generalizes to construct a κ -Aronszajn tree whenever $\kappa = \lambda^+$, λ is regular, and for all cardinals $\theta < \lambda$, $2^\theta \leq \lambda$ (in proving 4.9, make sure $\text{range}(s_\alpha)$ is non-stationary). In particular, under GCH, there is a κ -Aronszajn tree whenever κ is the successor of a regular cardinal. The situation for successors of singular cardinals is open under GCH*, although if $V = L$, there are κ -Aronszajn trees for such κ (Jensen — see Chapter B.5). It is consistent with $c = \omega_2$ that there are no ω_2 -Aronszajn trees (see MITCHELL [1972]). κ -Aronszajn trees for κ strongly inaccessible are discussed in Section 6.

Trees are very much related to total orders and the Suslin problem (see Section 3). In general, given a tree $(T, <)$, we may obtain a (strict) total order $\triangleleft$ of the points of T as follows. First, picture T written on the blackboard, rather than growing out of the ground. Then points on a given level are ordered from left to right. To compare points at different levels, we squash T down into the chalk bin, making sure that branches do not get squashed down above a point (Fig. 2). More formally, we call a total order $\triangleleft$ of T a *squashing* of $<$ iff

- (a) If b and c are at the same level of T , $b \leq d$, $c \leq g$, and $b \triangleleft c$, then $d \triangleleft g$, and
- (b) If $a < c < e$, then $a \triangleleft c$ iff $a \triangleleft e$.

Such a $\triangleleft$ is easy to construct by induction on the levels of T , but it is not unique; we are perfectly free to order the immediate successors of a point x any way we like, and the placement of x with respect to them is also completely arbitrary. We remark that if T is a sub-tree of some $2^{<\alpha}$, then the lexicographic order is a squashing of it.

4.10. THEOREM. *Let κ be regular, $(T, <)$ a κ -Aronszajn tree, and $\triangleleft$ a squashing of T . Then there are no strictly increasing or strictly decreasing κ -sequences in $(T, \triangleleft)$.*

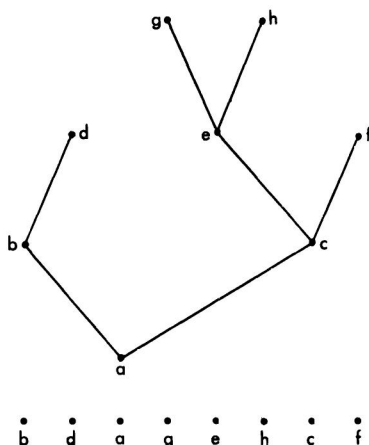


Fig. 2.

PROOF. Say $\langle x_\alpha : \alpha < \kappa \rangle$ were an increasing sequence. For each $\xi < \kappa$, define a point y_ξ on the ξ -th level as follows: Fix ξ , then fix α such that for all $\beta > \alpha$, x_β is at a level $> \xi$; for $\beta > \alpha$, let z_β be the element at level ξ below x_β ; then $\langle z_\beta : \alpha < \beta < \kappa \rangle$ is non-decreasing in $\triangleleft$, and hence eventually constant; let y_ξ be this constant value. Now $\{y_\xi : \xi < \kappa\}$ is a path through T , a contradiction. $\square$

Suslin trees are very nice Aronszajn trees. A squashed Suslin tree is (with a bit of fudging) a Suslin line. If one starts with a Suslin line, the method of proof of the Čech–Pospíšil theorem yields a Suslin tree.

More formally, an *antichain* in T is a set $A \subseteq T$ such that whenever x, y are distinct elements of A , $x \not\triangleleft y$ and $y \not\triangleleft x$. A κ -Suslin tree is a κ -Aronszajn tree with the property that T has no antichains of cardinality κ . Then

4.11. THEOREM. *There exists an ω_1 -Suslin tree iff there exists a Suslin line.*

PROOF. First, let $(T, <)$ be an ω_1 -Suslin tree. It is sufficient to produce a c.c.c. dense total order which is not separable, since its Dedekind completion (with the first and last elements removed) will then be a Suslin line.

Now, if $\triangleleft$ is any squashing of $(T, <)$, it almost works, except that it may be neither c.c.c. nor dense. To patch up density, call points x and y equivalent ($x \sim y$) iff there are at most countably many elements between them in $\triangleleft$. Let $L = T/\sim$ with the natural order, which we call also $\triangleleft$. Let $[x]$ be the equivalence class of x .

L is clearly dense in itself. To see that L is c.c.c. suppose $\mathcal{J}$ were an uncountable family of disjoint open intervals. If $([x], [y]) \in \mathcal{J}$, then there are uncountably many elements between x and y in $\triangleleft$, so we may inductively pick $x_\alpha, y_\alpha, z_\alpha$ ($\alpha < \omega_1$) so that $([x_\alpha], [y_\alpha]) \in \mathcal{J}$, $x_\alpha \triangleleft z_\alpha \triangleleft y_\alpha$, the level of z_α in T is above those of x_α and y_α , and the levels of x_α and y_α in T are above those of z_β for $\beta < \alpha$. Then $\{z_\alpha : \alpha < \omega_1\}$ would be an uncountable antichain in T .

To show that L is not separable, let $X \subset L$ be countable. Let α be above the levels of all elements of equivalence classes in X . If x is in the α -th level, $[x]$ and all equivalence classes of points above x in T define the same Dedekind cut in X , so at most two of these can be in the closure of X . Thus, the closure of X is countable.

The construction of the tree from the line is analogous to the proofs of 4.1 and 4.3. Let $(L, <)$ be a Suslin line. Let $L' = L \cup \{-\infty, +\infty\}$, ordered in the obvious way; then L' is compact. Now, by induction on $s \in 2^{<\omega_1}$ define closed (possibly degenerate) intervals, $[a_s, b_s] \subseteq L'$ ($a_s \leq b_s$). $[a_{\langle \rangle}, b_{\langle \rangle}] = L' = [-\infty, +\infty]$. If $a_s = b_s$, let $[a_{s \wedge 0}, b_{s \wedge 0}] = [a_{s \wedge 1}, b_{s \wedge 1}] = [a_s, b_s]$. If $a_s < b_s$, let $a_{s \wedge 1} = b_{s \wedge 0}$ be some point in (a_s, b_s) , $a_{s \wedge 0} = a_s$, and $b_{s \wedge 1} = b_s$; i.e., we split $[a_s, b_s]$ into two adjacent intervals. If $\text{lh } s$ is a limit, let $[a_s, b_s] = \bigcap \{[a_{s \upharpoonright \alpha}, b_{s \upharpoonright \alpha}]: \alpha < \text{lh } s\}$.

Let $T = \{s \in 2^{\omega_1}: a_s < b_s\}$. Then T is a subtree of $2^{<\omega_1}$, and we shall check that it is Suslin. First, for each $p \in L$, we can let $f_p: \omega_1 \rightarrow 2$ be chosen so that $\forall \alpha < \omega_1 (p \in [a_{f_p \upharpoonright \alpha}, b_{f_p \upharpoonright \alpha}])$. Since there can be no ω_1 -sequence of strictly nested intervals, there must be an α such that $a_{f_p \upharpoonright \alpha} = b_{f_p \upharpoonright \alpha} = p$; if α is least, let $s_p = f_p \upharpoonright \alpha$. Then $\text{lh}(s_p)$ is a limit, and for $\xi < \text{lh}(s_p)$, $s_p \upharpoonright \xi \in T$. Since

$$\{p\} = \bigcap \{[a_{s_p \upharpoonright \xi}, b_{s_p \upharpoonright \xi}]: \xi < \text{lh } s_p\},$$

$\{a_t: t \in T\} \cup \{b_t: t \in T\}$ is dense in L' , and hence uncountable; so T is uncountable. However, each antichain (and hence each level) of T is countable, since if A is an antichain, the (a_s, b_s) for $s \in A$ are disjoint. Finally, T is Aronszajn, since a path through T would yield an ω_1 -sequence of strictly nested intervals in L' . $\square$

By Theorems 3.8 and 4.11, $\diamond$ implies that there is an ω_1 -Suslin tree. One may also construct the tree directly using $\diamond$. It is this direct construction which is more useful in generalizations to larger cardinals (see Section 11 of Chapter B.5).

Although, in elementary topology, it is the line which has the most

obvious interest, the tree may be used directly to construct various topological spaces (see, e.g. RUDIN [1975]).

For more on trees in general, see JECH [1971].

5. Almost disjoint sets

Obviously, ω cannot be partitioned into more than ω pairwise disjoint sets. However, if we call $x, y \subseteq \omega$ *almost disjoint* iff $|x| = |y| = \omega$ and $|x \cap y| < \omega$, then

5.1. THEOREM. *There is a family $\mathcal{A} \subseteq \mathcal{P}(\omega)$ such that $|\mathcal{A}| = 2^\omega$ and the elements of $\mathcal{A}$ are pairwise almost disjoint.*

PROOF. The idea is that any two paths through the complete binary tree of height ω are almost disjoint. Thus, we shall take $\mathcal{A} \subseteq \mathcal{P}(2^{<\omega})$. If $f \in 2^\omega$, let $a_f = \{f \upharpoonright n : n \in \omega\}$. Let $\mathcal{A} = \{a_f : f \in 2^\omega\}$.

Generalizations to larger cardinals depend on the axioms of set theory. If $x, y \subseteq \kappa$, call x, y *almost disjoint* iff $|x| = |y| = \kappa$ but $|x \cap y| < \kappa$. To repeat the above argument, we would need that the tree $2 < \kappa$ has cardinality only κ , which may be false. In fact, the existence of a family of 2^{ω_1} almost disjoint subsets of ω_1 is consistent with and independent from $\text{ZFC} + 2^\omega = 2^{\omega_1} = \omega_3$.

The method in 5.1 may actually be used to prove statements about the behavior of the cardinal exponentiation function at singular cardinals. It is consistent with ZFC that $\exp$ on regular cardinals be anything not patently absurd (e.g., $\exp(\omega) = \omega_{\omega_1}$, $\exp(\omega_1) = \exp(\omega_2) = \omega_{\omega_1+35}$, etc. is consistent — see EASTON [1970] or Theorem 5.9 of Chapter B.4, but at singular cardinals the situation is more obscure. It is open whether it is consistent that GCH first fails at ω_ω (i.e. $\forall n < \omega [\exp(\omega_n) = \omega_{n+1}]$ but $\exp(\omega_\omega) \geq \omega_{\omega+2}$). However, this cannot happen at ω_{ω_1} — i.e.:

5.2. THEOREM (Silver). *If $\forall \alpha < \omega_1 (\exp(\omega_\alpha) = \omega_{\alpha+1})$, then $\exp(\omega_\omega) = \omega_{\omega_1+1}$.*

Silver's proof used metamathematical ideas outside the scope of this paper. We present a direct combinatorial proof due independently to Baumgartner, Jensen and Prikry.

The appropriate generalization of 5.1 uses almost disjoint functions:

5.3. LEMMA. Assume $\forall \alpha < \omega_1 (\exp(\omega_\alpha) = \omega_{\alpha+1})$. Then there is an $\mathcal{F} \subset (\omega_{\omega_1})^{\omega_1}$ such that

- (a) $\forall f, g \in \mathcal{F} (f \neq g \rightarrow \exists \alpha < \omega_1 \forall \beta > \alpha (f(\beta) \neq g(\beta)))$.
- (b) $\forall f \in \mathcal{F} \forall \alpha < \omega_1 (f(\alpha) < \omega_{\alpha+1})$.
- (c) $|\mathcal{F}| = \exp(\omega_{\omega_1})$.

PROOF. For $\alpha < \omega_1$, fix a 1-1 map φ_α from $\mathcal{P}(\omega_\alpha)$ into $\omega_{\alpha+1}$. If $X \subseteq \omega_{\omega_1}$, let $f_x(\alpha) = \varphi_\alpha(X \cap \omega_\alpha)$. Let $\mathcal{F} = \{f_x : X \subseteq \omega_{\omega_1}\}$. $\square$

We now attempt to bound $|\mathcal{F}|$. If (b) were replaced by $f(\alpha) < \omega_\alpha$, a bound would result from the pressing-down lemma (2.3). More generally:

5.4. LEMMA. Assume $\forall \alpha < \omega_1 (\exp(\omega_\alpha) = \omega_{\alpha+1})$. Let $\mathcal{F}$ satisfy 5.3 (a) plus
(b') $\forall f \in \mathcal{F} (\{\alpha : f(\alpha) < \omega_\alpha\} \text{ is stationary})$.

Then $|\mathcal{F}| \leq \omega_{\omega_1}$.

PROOF. For $f \in \mathcal{F}$, define $f^* : \omega_1 \rightarrow \omega_1$ so that $|f(\alpha)| = \omega_{f^*(\alpha)}$. Then $\{\alpha : f^*(\alpha) < \alpha\}$ is stationary, so by 2.3 there is a $\beta_f < \omega_1$ and a stationary $S_f \subset \omega_1$ with $\forall \alpha \in S_f (f^*(\alpha) = \beta_f)$. Now there are only ω_1 possibilities for β_f and ω_2 possibilities for S_f . Furthermore, for each fixed β and S ,

$$|\{f \in \mathcal{F} : \beta_f = \beta \ \& \ S_f = S\}| \leq \omega_{\beta+2},$$

since the $f \upharpoonright S$ are distinct (by (a)) functions into $\omega_{\beta+1}$. Thus, $|\mathcal{F}| \leq \omega_{\omega_1}$. $\square$

Lemma 5.4 may be generalized to:

5.5. LEMMA. Assume $\forall \alpha < \omega_1 (\exp(\omega_\alpha) = \omega_{\alpha+1})$. Let $g : \omega_1 \rightarrow \omega_{\omega_1}$ be such that $\forall \alpha (g(\alpha) < \omega_{\alpha+1})$. Let $\mathcal{F}$ satisfy 5.3 (a) plus

- (b'') $\forall f \in \mathcal{F} (\{\alpha : f(\alpha) < g(\alpha)\} \text{ is stationary})$.

Then $|\mathcal{F}| \leq \omega_{\omega_1}$.

PROOF. For $\alpha < \omega_1$, fix a 1-1 map ψ_α from $g(\alpha)$ into ω_α . Let $f'(\alpha)$ be $\psi_\alpha(f(\alpha))$ when $f(\alpha) < g(\alpha)$ and $f(\alpha)$ when $f(\alpha) \geq g(\alpha)$, and apply 5.4 to $\{f' : f \in \mathcal{F}\}$. $\square$

Now, let $\mathcal{F}$ be as in 5.3. We complete the proof of 5.2 by showing $|\mathcal{F}| = \omega_{\omega_1+1}$. For g and f distinct members of $\mathcal{F}$, we say $g < f$ a.e. iff $\{\alpha : f(\alpha) < g(\alpha)\}$ is not stationary — i.e., $\{\alpha : g(\alpha) < f(\alpha)\}$ contains a c.u.b. subset. Then 5.5 says that for any $g \in \mathcal{F}$, $g < f$ a.e. for all but at most ω_{ω_1} members f of $\mathcal{F}$. We may thus inductively pick $f_\mu \in \mathcal{F}$ for $\mu < \omega_{\omega_1+1}$ so that

$\mu < \nu \rightarrow f_\mu < f_\nu$ a.e. Let $\mathcal{F}_\mu = \{g \in \mathcal{F} : g < f_\mu \text{ a.e.}\}$. By 5.5, $\bigcup \{\mathcal{F}_\mu : \mu < \omega_{\omega_1+1}\} = \mathcal{F}$, but again by 5.5, each $|\mathcal{F}_\mu| \leq \omega_{\omega_1}$. Thus $|\mathcal{F}| = \omega_{\omega_1+1}$. $\square$

Theorem 5.2 easily generalizes to:

5.6. THEOREM. *If $\omega < \text{cf}(\lambda) < \lambda$ and $\{\kappa < \lambda : \exp(\kappa) = \kappa^+\}$ is stationary in λ , then $\exp(\lambda) = \lambda^+$.*

For further generalizations, see GALVIN and HAJNAL [1975].

A concept related to almost disjoint families is that of quasi-disjointness. A family $\mathcal{A}$ of sets is *quasi-disjoint*, or forms a Δ -system (see Fig. 3) iff there is a fixed b such that $a \cap a' = b$ whenever a and a' are distinct members of $\mathcal{A}$. b is called the *root* of $\mathcal{A}$. The following “ Δ -system lemma” is frequently used in topology and combinatorics.

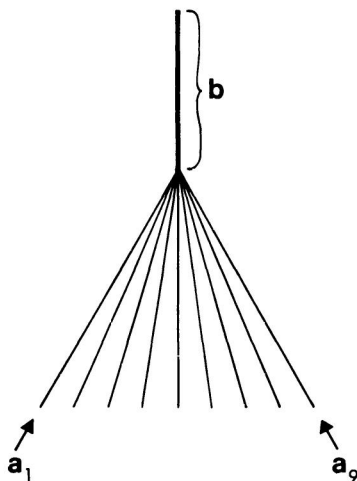


Fig. 3.

5.7. THEOREM. *If $\mathcal{A}$ is an uncountable family of finite sets, there is an uncountable $\mathcal{B} \subset \mathcal{A}$ which is quasi-disjoint.*

PROOF. Since there are only ω finite cardinals, we may assume that all the members of $\mathcal{A}$ have cardinality n for some fixed n . We proceed by induction on n . If $n = 1$, 5.7 is trivial. If $n = m + 1$ where $m \geq 1$, we consider two cases.

Case I. Some element p is contained in uncountably many members of $\mathcal{A}$. Apply the inductive hypothesis to $\{a - \{p\} : a \in \mathcal{A} \text{ and } p \in a\}$.

Case II. Not case I. Inductively pick $a_\alpha \in \mathcal{A}$ ($\alpha < \omega_1$) so that $a_\alpha \cap a_\xi = \emptyset$ for all $\xi < \alpha$. Let $\mathcal{B} = \{a_\alpha : \alpha < \omega_1\}$. $\square$

For generalizations of 5.7 to other cardinalities, see JUHÁSZ [1971].

We present an elementary topological application of 5.7. A space X is called *c.c.c.* iff there are no uncountable families of pairwise disjoint open sets in X . So $\mathbb{R}^n$ is *c.c.c.* for all n . A Suslin line (if it exists — see Section 3) is *c.c.c.* but its square is not. It is consistent with set theory that any product of *c.c.c.* spaces is *c.c.c.* (see Chapter B.6). The following shows that, regardless of the axioms of set theory, it is sufficient to look at finite products; it implies immediately that $\mathbb{R}^\kappa$ is *c.c.c.* for all κ .

5.8. THEOREM. *If X_i ($i \in I$) are spaces and $\prod_{i \in I} X_i$ is not *c.c.c.*, then there is a finite $b \subseteq I$ with $\prod_{i \in b} X_i$ not *c.c.c.**

PROOF. Say V_α ($\alpha < \omega_1$) are pairwise disjoint basic open sets in the product. Each V_α depends only on a finite set of coordinates, $a_\alpha \subset I$. By 5.7, let T be an uncountable subset of ω_1 such that $\{a_\alpha : \alpha \in T\}$ form a Δ -system with root b . Let V_α^* be the projection of V_α in $\prod_{i \in b} X_i$. Then the V_α^* ($\alpha \in T$) are disjoint, so $\prod_{i \in b} X_i$ is not *c.c.c.* $\square$

6. Partition calculus

Intuitively, a graph is a set of points in space, some of which are connected by lines (see Fig. 4). Formally, let $[I]^2 = \{\{x, y\} : x, y \in I \text{ \& } x \neq y\}$. Then a graph is a pair, $(I, \mathcal{E})$ where $\mathcal{E} \subseteq [I]^2$. Thus, in Fig. 4A, $I = 4$ and $\mathcal{E} = \{\{0, 1\}, \{1, 3\}, \{1, 2\}\}$. $(I', \mathcal{E}')$ is a *subgraph* of $(I, \mathcal{E})$ iff $I' \subseteq I$ and $\mathcal{E}' = \mathcal{E} \cap [I']^2$; so graph A is a subgraph of graph C. The *complete graph* on I is $(I, [I]^2)$. The *empty graph* on I is $(I, \emptyset)$.

A special case of the finite version of Ramsey's theorem is that if a graph has 6 or more points, then it either has a 3-point empty subgraph (e.g. $\{1, 4, 5\}$ in C) or a 3-point complete subgraph (e.g. $\{0, 1, 2\}$ in D). Graph B shows that this can fail for graphs with only 5 points. The reader is invited to construct a proof that 6 is large enough.

More generally, Ramsey showed that for each $j \in \omega$, there is an $i \in \omega$ such that whenever $(I, \mathcal{E})$ has at least i points, it has either a complete or an empty subgraph with j points. Call $R(j)$ the least i that works; so $R(2) = 2$ and $R(3) = 6$. Unfortunately, there is no nice formula for $R(j)$. Fortu-

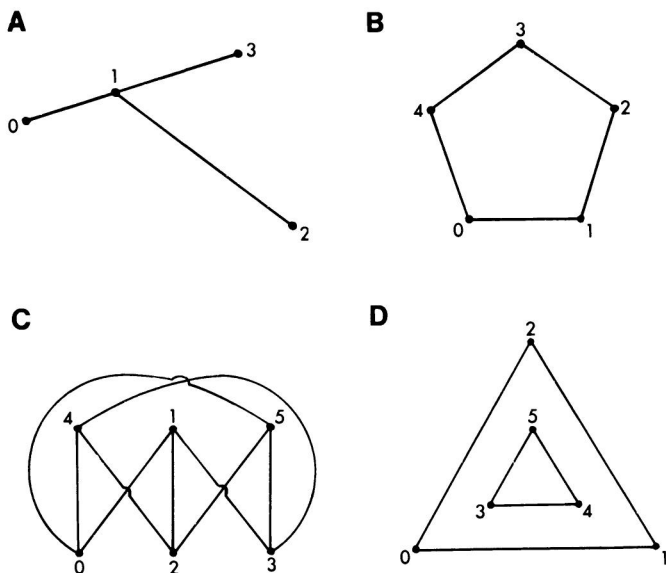


Fig. 4.

nately, however, infinite combinatorics is much simpler than finite combinatorics; $R(\omega)$ is exactly ω and R of most other infinite cardinals can be computed explicitly in terms of cardinal arithmetic.

The above notions may be generalized in two ways.

First, if σ is a cardinal, a function $P : [I]^2 \rightarrow \sigma$ is called a *partition* of $[I]^2$ into σ pieces. We may think of P as coloring each of the edges of the complete graph on I in one of σ possible colors. Graphs then in the previous sense may be thought of as partitions of $[I]^2$ into two pieces; e.g. in Fig. 4A, the edges $\{0, 1\}$, $\{1, 3\}$, $\{1, 2\}$ are colored black and the other three edges are colored white (so they do not show).

Second, we may consider $[I]^n = \{F \subseteq I : |F| = n\}$ and partitions $P : [I]^n \rightarrow \sigma$.

If $P : [I]^n \rightarrow \sigma$, we call $H \subseteq I$ *homogeneous* for P iff P is constant on $[H]^n$. The Erdős notation $\kappa \rightarrow (\lambda)_\sigma^n$ is used to abbreviate the assertion: Whenever $P : [\kappa]^n \rightarrow \sigma$, there is an $H \subseteq \kappa$ homogeneous for P of cardinality λ . So, e.g., $6 \rightarrow (3)_2^2$ but $5 \not\rightarrow (3)_2^2$. Note that if $\kappa \rightarrow (\lambda)_\sigma^n$, $\kappa' \geq \kappa$, $\lambda' \leq \lambda$, $\sigma' \leq \sigma$, and $n' \leq n$, then $\kappa' \rightarrow (\lambda')_{\sigma'}^{n'}$.

The finite version of Ramsey's theorem, which we shall not prove, is that for each $n, \sigma, \lambda \in \omega$, there is a $\kappa \in \omega$ such that $\kappa \rightarrow (\lambda)_\sigma^n$. The question of how small a κ will work is still a subject of much research (see ERDŐS,

HAJNAL and RADO [1965]). In the following, κ and λ will always be infinite cardinals. Incidentally, ERDŐS and RADO [1952] showed that for all κ , $\kappa \not\rightarrow (\omega)_2^\omega$, so n will always be finite (if one drops the axiom of choice, relations like $\kappa \rightarrow (\lambda)_2^\omega$ may be consistent — see, e.g., KLEINBERG [1970]).

We shall show that for any n, σ, λ there is a κ such that $\kappa \rightarrow (\lambda)_\sigma^n$, and in many cases produce a formula giving the least such κ . Our first result is

6.1. THEOREM (Ramsey). $\omega \rightarrow (\omega)_\sigma^n$ for any $n, \sigma \in \omega$.

The first non-trivial case of 6.1 is $\omega \rightarrow (\omega)_2^2$, the fact stated above for graphs. We defer the proof of 6.1 until after we discuss the situation for larger cardinals, since a number of related results can be proved by the same method.

If one replaces ω by ω_1 in 6.1, the theorem becomes false by either (a) or (b) of the following (with $\kappa = \omega$).

6.2. THEOREM. For any κ

- (a) $2^\kappa \not\rightarrow (3)_\kappa^2$,
- (b) $2^\kappa \not\rightarrow (\kappa^+)_2^2$.

PROOF. For (a), identify 2^κ with the set of functions from κ into 2, and define $P(\{f, g\})$ to be the least α such that $f(\alpha) \neq g(\alpha)$.

For (b), it is convenient to prove first:

6.3. LEMMA. If $\kappa \rightarrow (\lambda)_2^2$ and $(L, <)$ is a total ordering of cardinality κ , then there is either an increasing or a decreasing λ -sequence in L .

PROOF. Let $\triangleleft$ be any well-ordering of L , and define $P: [L]^2 \rightarrow 2$ by $P(\{x, y\}) = 0$ iff $<$ and $\triangleleft$ agree on $\{x, y\}$. Then a homogeneous set for P of size λ gives the desired sequence.

To prove (b) from the lemma, it is sufficient to produce an order of cardinality 2^κ with no increasing or decreasing κ^+ -sequences. If $\kappa = \omega$, the real numbers will do. In general, let L be the set of functions from κ into 2 and order L lexicographically; that this has the desired property may be proved exactly like 4.10. $\square$

If one goes to $(2^\kappa)^+$, one gets positive results in 6.2 — i.e., $(2^\kappa)^+ \rightarrow (\kappa^+)_\kappa^2$. More generally, let $\exp_0(\kappa) = \kappa$; $\exp_{n+1}(\kappa) = 2^{\exp_n(\kappa)}$. Then:

6.4. THEOREM (ERDŐS and RADO [1956]). For every κ and all $n \geq 1$, $(\exp_{n-1}(\kappa))^+ \rightarrow (\kappa^+)_\kappa^n$.

We shall prove 6.4 later, but we state without proof the assertion that it is the best possible. A proof may be extracted from ERDÖS, HAJNAL and RADO [1965].

6.5. THEOREM. *For all $n \geq 1$,*

- (a) $\exp_{n-1}(\kappa) \not\rightarrow (\kappa^+)_2^n$,
- (b) $\exp_{n-1}(\kappa) \not\rightarrow (n+2)_\kappa^n$.

By 6.4, for any n, σ, λ there is a κ such that $\kappa \rightarrow (\lambda)_\sigma^n$. For some cases — e.g. when λ is a successor and $\sigma < \lambda$, 6.4 and 6.5 give the best such κ . One can establish the best κ for most other cases (see ERDÖS, HAJNAL and RADO [1965]), but the results seem too tedious to state here. A more interesting question is whether κ can be λ . The first non-trivial possibility, $\kappa \rightarrow (\kappa)_2^2$, leads immediately to larger cardinals.

6.6. THEOREM. *If $\kappa \rightarrow (\kappa)_2^2$ and $\kappa > \omega$, then κ is strongly inaccessible.*

PROOF. By 6.2(b), if $\lambda < \kappa$, then $2^\lambda \not\rightarrow (\lambda^+)_2^2$, whereas since $\lambda^+ \leq \kappa$, $\kappa \rightarrow (\lambda^+)_2^2$; thus, $2^\lambda < \kappa$. If κ were not regular, write $\kappa = \bigcup_{\xi < \alpha} A_\xi$, where the A_ξ are disjoint, $\alpha < \kappa$, and each $|A_\xi| < \kappa$. Define $P : [\kappa]^2 \rightarrow 2$ so that $P(\{x, y\}) = 0$ iff x and y are in the same A_ξ . Then P could have no homogeneous set of size κ . $\square$

In fact, $\kappa \rightarrow (\kappa)_2^2$ implies that κ is the κ -th strong inaccessible (see Section 7).

There now comes to mind a whole spectrum of properties: $\kappa \rightarrow (\kappa)_3^2$, $\kappa \rightarrow (\kappa)_2^3$, etc. Fortunately, these are all the same.

6.7. THEOREM. *If $\kappa \rightarrow (\kappa)_2^2$, then $\kappa \rightarrow (\kappa)_\sigma^n$ for all $n < \omega$ and all $\sigma < \kappa$.*

We now owe the reader three proofs: 6.1, 6.4, and 6.7. We have been postponing them because they are all so similar they can just as well be done simultaneously. The similarity is in four respects. First, they are all proved by induction on n . Second, they are all trivial for $n = 1$.

Third, they all use the concept of a *pre-homogeneous* (p.h.) set in the induction step. If $P : [\theta]^{n+1} \rightarrow \sigma$ and $H \subseteq \theta$, we call H p.h. for P iff P on $[H]^{n+1}$ does not depend on the last element of an $(n+1)$ -tuple — i.e. $P(\{x_1, \dots, x_n, y\}) = P(\{x_1, \dots, x_n, z\})$ whenever $x_1 < x_2 < \dots < x_n$, $x_n < y$, $x_n < z$, and $x_1, \dots, x_n, y, z \in H$. If H is p.h. for P and H has no last element, then we can define $Q : [H]^n \rightarrow \sigma$ by letting $Q(\{x_1, \dots, x_n\}) =$

$P(\{x_1, \dots, x_n, y\})$ for some (any) $y \in H$ larger than $x_1, \dots, x_n$. If $K \subseteq H$ is homogeneous for Q , then K is homogeneous for P . Thus, the existence of a large p.h. set, plus an inductive assumption about partitions of n -tuples will imply a partition relation for $n+1$ -tuples. More precisely, Theorems 6.1, 6.4, and 6.7 follow by induction from parts (a), (b), and (c) respectively of

6.8. LEMMA. *Let $n \geq 1$.*

(a) *If $P: [\omega]^{n+1} \rightarrow \sigma$, where $\sigma < \omega$, then there is an infinite p.h. set for P .*

(b) *If $P: [\theta]^{n+1} \rightarrow \sigma$, and $\theta > \sigma^{<\lambda}$, then there is a p.h. set for P of cardinality λ .*

(c) *If $P: [\kappa]^{n+1} \rightarrow \sigma$, where $\sigma < \kappa$ and $\kappa \rightarrow (\kappa)_2^2$, then there is a p.h. set for P of cardinality κ .*

Note that in proving 6.4, (b) is used for $\theta = (\exp_n(\kappa))^+$, $\lambda = (\exp_{n-1}(\kappa))^+$, and $\sigma = \kappa$; one assumes inductively that $(\exp_{n-1}(\kappa))^+ \rightarrow (\kappa^+)_\kappa^n$. (b) is useful in deriving other partition relations not covered by our stated theorems; for example, if κ is strongly inaccessible, then $\kappa^+ \rightarrow (\kappa)_\sigma^2$ for any $\sigma < \kappa$ (take $\theta = \kappa^+$, $\lambda = \kappa$). It is probably better to remember the proof of 6.8 (to follow), rather than a collection of seemingly unrelated arrow relations.

The fourth similarity in our proofs is that the desired p.h. set will arise from a path through a tree. 6.8 (a) will use König's lemma (4.7) that there are no ω -Aronszajn trees. 6.8(b) will use a direct cardinality argument. 6.8(c) will use König's lemma at κ , namely:

6.9. LEMMA. *If $\kappa \rightarrow (\kappa)_2^2$, there are no κ -Aronszajn trees.*

PROOF. By Theorem 4.10, a κ -Aronszajn tree may be squashed to a total ordering of size κ with no increasing or decreasing κ -sequences. But then by 6.3, $\kappa \not\rightarrow (\kappa)_2^2$. $\square$

We now prove Lemma 6.8 for the case $n = 1$. The general situation is: we are given a partition $P: [\theta]^2 \rightarrow \sigma$ and we wish to produce a p.h. set of size λ . We shall define a subtree T of the complete σ -ary tree $\sigma^{<\lambda}$ and a function $h: T \rightarrow \theta$ in such a way that if $f: \lambda \rightarrow \sigma$ is a path through T , $\{h(f \upharpoonright \xi): \xi < \lambda\}$ will be a p.h. set for P , enumerated in increasing order; further, the Q defined above 6.8 will be given by f (i.e., $Q(\{h(f \upharpoonright \xi)\}) = f(\xi)$). So T is the tree of potential Q 's and h assigns potential p.h. sets to members of T .

More formally, define, for all $s \in \sigma^{<\lambda}$, $h(s) \in \theta$ and $A(s) \subseteq \theta$ so that:

(i) $A(\langle \rangle) = \theta$.

(ii) $h(s)$ is the least element of $A(s)$ if $A(s) \neq 0$; if $A(s) = 0$, say $h(s) = 0$ (this will be irrelevant).

(iii) If $lh(s)$ is a limit, $A(s) = \bigcap \{A(s \upharpoonright \xi) : \xi < lh(s)\}$.

(iv) $A(s^\wedge \mu) = A(s) \cap \{\gamma > h(s) : P(\{h(s), \gamma\}) = \mu\}$.

Let $T = \{s : A(s) \neq 0\}$. Now if $f : \lambda \rightarrow \sigma$ is such that $\forall \xi < \lambda (f \upharpoonright \xi \in T)$, then for all $\xi < \eta < \lambda$, $h(f \upharpoonright \eta) \in A(f \upharpoonright (\xi + 1))$, so $P(\{h(f \upharpoonright \xi), h(f \upharpoonright \eta)\}) = f(\xi)$; thus $\{h(f \upharpoonright \xi) : \xi < \lambda\}$ will be p.h. as desired. To see that there is such an f , note that if $\gamma < \theta$ is not equal to $h(s)$ for any $s \in \sigma^{<\lambda}$, one may define an f inductively so that $\gamma \in A(f \upharpoonright \xi)$ for all ξ — this can be done since the only element of $A(s)$ not in $\bigcup \{A(s^\wedge \mu) : \mu < \sigma\}$ is $h(s)$. Thus, we are done when the cardinal $\sigma^{<\lambda}$ is less than θ , so 6.8(b) is proved (for $n = 1$). In the case of 6.8(a) and (c), θ is inaccessible or ω and $\lambda = \theta$, so $\sigma^{<\lambda} = \theta$, but $\sigma^{<\alpha} < \theta$ for all $\alpha < \theta$; our argument now only shows that the tree has height θ , since for $\alpha < \theta$, we may fix a γ not equal to $h(s)$ for any s of length $< \alpha$, and produce an f of length α with $\gamma \in A(f)$. Thus, if there are no paths through T , T would be a θ -Aronszajn tree, so 6.8(a) and (c) (for $n = 1$) follows from König's lemma and 6.9 respectively.

To prove 6.8 for arbitrary $n \geq 1$, we work not with $\sigma^{<\lambda}$, but with the tree of potential partitions of n -tuples. Let, for $\xi < \lambda$, $S_\xi^n = \{s : s : [\xi]^n \rightarrow \sigma\}$. Then S_ξ^n is the ξ -th level of the tree $S^n = \bigcup \{S_\xi^n : \xi < \lambda\}$, where $s \leq t$ iff $s \subseteq t$. So, for $n = 1$, S^n may be identified with $\sigma^{<\lambda}$. Given $P : [\theta]^{n+1} \rightarrow \sigma$, define, for $s \in S^n$, $h(s) \in \theta$ and $A(s) \subseteq \theta$ so that

(i) $A(0) = \theta$.

(ii) $h(s)$ is the least element of $A(s)$ if $A(s) \neq 0$; if $A(s) = 0$ let $h(s) = 0$.

(iii) If $s \in S_\eta^n$ for limit η , $A(s) = \bigcap \{s \upharpoonright [\xi]^n : \xi < \eta\}$.

(iv) If $s \in S_\xi^n$, $t \in S_{\xi+1}^n$, and $s \leq t$,

$$A(t) = A(s) \cap \{\gamma > h(s) : \forall F \in [\xi + 1]^n (P(h(F) \cup \{\gamma\}) = t(F))\}.$$

In (iv), $h(F)$ means $\{h(t \upharpoonright [\eta_1]^n), h(t \upharpoonright [\eta_2]^n), \dots, h(t \upharpoonright [\eta_n]^n)\}$, where $F = \{\eta_1 \cdots \eta_n\}$. With these definitions, the proof for arbitrary n proceeds as before. $\square$

We have thus proved 6.8, and hence Theorems 6.1, 6.4, and 6.7. A review of our argument for 6.7 shows that we have in fact established:

6.10. THEOREM. *Let $\kappa > \omega$. Then the following are equivalent:*

(i) $\kappa \rightarrow (\kappa)_2^2$.

(ii) $\kappa \rightarrow (\kappa)_\sigma^n$ for all $n < \omega$ and all $\sigma < \kappa$.

(iii) κ is strongly inaccessible and there are no κ -Aronszajn trees.

(iv) *Whenever $(L, <)$ is a total ordering of size κ , there is either an increasing or a decreasing κ -sequence in L .*

PROOF. (ii) $\rightarrow$ (i) is trivial. (i) $\rightarrow$ (iv) is Lemma 6.3. The proof of 6.9 establishes (iv) $\rightarrow$ (iii) if we can see that (iv) implies that κ is strongly inaccessible. To see this, look back at the proof of 6.6. The proof that $\lambda < \kappa$ implies $2^\lambda < \kappa$ is unchanged. If κ were not regular, we could, following the notation of 6.6, define an order $\triangleleft$ on κ by saying $x \triangleleft y$ iff either $x < y$ and x, y are in the same A_ξ , or $x \in A_\xi$, $y \in A_\eta$ where $\xi > \eta$. Then there could be no increasing or decreasing κ -sequences in $(\kappa, \triangleleft)$. Finally, our proof of 6.7 establishes (iii) $\rightarrow$ (i). $\square$

The text ERDŐS, HAJNAL, MÁTÉ and RADO [~1977] contains κ more theorems on the partition calculus.

7. Large cardinals

Mathematicians and other children often play the following game: We take turns naming numbers, and see who can name the largest one. This is a game in the psychological rather than in the formal sense, since I might always just add one to your number, but my goal is to try to completely demolish your ego by transcending your number via some completely new principle. Thus, a sequence of plays might be:

me: XVII,
 you: 1,295,387,
 me: $10^{10^{10}}$,
 you: ω ,
 me: $\omega_{(\omega_\omega)}$,
 ...

The next stages in the game, which are the subject of this section, go through various inaccessibility properties. Here we must distinguish between the weak and the strong properties. For example, κ is a (weak) limit cardinal iff $\lambda^+ < \kappa$ whenever $\lambda < \kappa$; it is a strong limit iff $2^\lambda < \kappa$ whenever $\lambda < \kappa$. κ is weakly inaccessible iff it is a regular limit cardinal $> \omega$, and strongly inaccessible iff it is a regular strong limit cardinal $> \omega$. Under GCH the weak and strong properties are equivalent, but it is consistent that there are weak inaccessibles $< 2^\omega$.

After you have played the first inaccessible, it would not take much imagination on my part to play the second, so instead I play the first hyper-inaccessible. Here, κ is (weakly/strongly) hyper-inaccessible iff κ is regular and a limit of (weak/strong) inaccessible cardinals. The notions of hyper-hyper-inaccessible, etc., are then obvious, so your honor demands that you play the first Mahlo cardinal.

We call κ *weakly Mahlo* iff $\kappa > \omega$, κ is regular, and the regular cardinals $< \kappa$ are stationary in κ . κ is *strongly Mahlo* iff κ is weakly Mahlo and strongly inaccessible.

7.1. LEMMA. *If κ is (weakly/strongly) Mahlo, then $\{\alpha < \kappa : \alpha \text{ is (weakly/strongly) inaccessible}\}$ is stationary in κ .*

PROOF. Note that $\{\alpha < \kappa : \alpha \text{ is (weak/strong) limit cardinal}\}$ is c.u.b. in κ , and that the intersection of a c.u.b. set and a stationary set is stationary. $\square$

It is now easy to see that in 7.1 we may replace “inaccessible” by “hyper-inaccessible” or “hyper-hyper-inaccessible.”

There is now a notion of hyper-Mahlo obtained by demanding that the set of Mahlo cardinals below κ be stationary in κ , and there is the obvious extension to hyper-hyper-Mahlo, etc., so I shall utterly annihilate you by naming the first weakly compact cardinal.

κ is called *weakly compact* iff $\kappa > \omega$ and $\kappa \rightarrow (\kappa)_2^2$. In 6.10, we proved various combinatorial equivalences to this notion. It is also equivalent to various statements in logic involving infinite formulas of length $< \kappa$ (see, e.g., BARWISE [1975]).

It is not immediate that weak compactness is a large cardinal property, although we know (6.6) that it does imply strong (sic) inaccessibility (unfortunately, “strongly compact” has been used for another notion — see the Appendix or DRAKE [1974]). However:

7.2. THEOREM. *If κ is weakly compact, then κ is strongly hyper-hyper-Mahlo.*

It is convenient to first prove:

7.3. THEOREM. *If κ is weakly compact and S any stationary subset of κ , then there is a regular $\lambda < \kappa$ such that $S \cap \lambda$ is stationary in λ .*

To deduce 7.2 from 7.3, first apply 7.3 with S any c.u.b. subset of κ to obtain a regular $\lambda \in S$; so κ is strongly Mahlo. Now, let $S_1 = \{\lambda < \kappa : \lambda \text{ is strongly inaccessible}\}$. If C is any c.u.b. subset of κ , we may apply 7.3 with $S = S_1 \cap C$ to get a regular $\lambda \in C$ with $S_1 \cap \lambda$ stationary in λ (i.e. λ is strongly Mahlo), so the set of strong Mahlo cardinals is stationary in κ . We may now replace S_1 by $S_2 = \{\lambda < \kappa : \lambda \text{ is strongly Mahlo}\}$ in the previous sentence to obtain that κ is strongly hyper-hyper-Mahlo.

To prove 7.3, we may first assume that S contains only infinite cardinals. Let $f : \kappa \rightarrow \kappa$ be the 1-1 increasing function that enumerates S . Let

$$T = \{s \in \kappa^{<\kappa} : \forall \xi < \text{lh}(s) [s(\xi) < f(\xi)] \text{ and } s \text{ is 1-1}\}.$$

T is a sub-tree of $\kappa^{<\kappa}$. If T had height κ , T would be a κ -Aronszajn tree, since a path through T would yield a 1-1 pressing-down function on S , contradicting 2.3. However, by 6.10, there are no κ -Aronszajn trees, so 7.3 follows from:

7.4. LEMMA. *Let A be any set of infinite cardinals such that for all regular λ , $A \cap \lambda$ is not stationary in λ . Then there is a 1-1 function g on A with $\forall \alpha \in A [G(\alpha) < \alpha]$.*

PROOF. Let $\gamma = \sup(A)$ and assume 7.4 holds for all A' with smaller sup. Then we have three cases:

Case I. γ is a successor cardinal. Trivial.

Case II. γ is singular: Let $\theta = \text{cf}(\gamma)$ and let δ_μ ($\mu < \theta$) be a continuously increasing cofinal sequence in γ , with each δ_μ a cardinal and $\delta_0 > \theta$. Let $g_\mu : A \cap \delta_\mu \rightarrow \delta_\mu$ satisfy 7.4. Define $g : A \rightarrow \gamma$ by

$$g(\alpha) = \begin{cases} g_0(\alpha) + 1 & \text{if } \alpha < \delta_0, \\ \delta_\mu + g_{\mu+1}(\alpha) & \text{if } \delta_\mu < \alpha < \delta_{\mu+1}, \\ \omega \cdot \mu & \text{if } \alpha = \delta_\mu. \end{cases}$$

Case III. γ is a regular limit cardinal. Proceed as in Case II (with $\theta = \gamma$), but make sure that $\delta_\mu \notin A$ for all μ .

It might be suspected that the conclusion of 7.3 is equivalent to weak compactness, but this turns out to be both consistent with (Jensen — see Theorem 14.2 of Chapter B.5), and independent from (KUNEN [$\sim$ 1977]) ZFC + GCH (see Section 3 of Chapter B.3).

Weakly compact cardinals are the beginning, not the end, of large cardinal theory. This game has been played to much greater heights (see SILVER [1973], SHOENFIELD [1971], SOLOVAY, REINHARDT and KANAMORI

[~ 1977]). It should be pointed out that it is cheating to name a number that does not exist. At times in the past, plausible large cardinal assumptions have turned out to be inconsistent with ZFC (KUNEN [1971]). Weakly compact cardinals are not known to be inconsistent with ZFC. But maybe ZFC is inconsistent.

Appendix*. Ridiculously large cardinals

Given an interesting property P of cardinal numbers κ , we investigate whether or not $P(\kappa)$ holds for some, most, or all cardinals κ . The results discussed in this chapter all take this form, where P is a combinatorial property. Sometimes we discover that a particular property $P(\kappa)$, like $\kappa \rightarrow (\kappa)_2^2$, is extremely rare, in that the least κ such that $P(\kappa)$ holds is incredibly large, so large in fact that we cannot even prove, from the usual axioms of set theory, that there is a κ such that $P(\kappa)$. In this case the statement “there is a cardinal κ such that $P(\kappa)$ ” is called a *large cardinal hypothesis*, at least until it is refuted.

All of the large cardinal hypotheses discussed in Section 7 of this chapter can be given more or less convincing justifications along the lines discussed at the end of Chapter B.1 — convincing enough, at any rate, that almost no one expects them to be refuted.

There are other, more problematic, large cardinal hypotheses. For these there is as yet no convincing justification. Far from being refuted, however, these hypotheses have led to some extremely beautiful mathematics. This work has been very well described in the literature, so we shall only indicate the directions taken, and point to the appropriate references in the references below.

Two large cardinal hypotheses which can be directly motivated as strengthenings of weak compactness are the Ramsey cardinal and the ineffable cardinal hypotheses. By $\kappa \rightarrow (\lambda)_{\sigma}^{<\omega}$ we mean that whenever we are given $\langle P_n : n \in \omega \rangle$ with $P_n : [\kappa]^n \rightarrow \sigma$, there is an $H \subseteq \kappa$ of cardinality λ which is homogeneous for each P_n . κ is a *Ramsey cardinal* iff $\kappa \rightarrow (\kappa)_2^{<\omega}$; this is equivalent to $\kappa \rightarrow (\kappa)_{\sigma}^{<\omega}$ for all $\sigma < \kappa$. By $\kappa \rightarrow (\text{stat})_{\sigma}^2$ we mean that whenever $P : [\kappa]^2 \rightarrow \sigma$, there is a stationary homogeneous set for P . κ is *ineffable* iff $\kappa \rightarrow (\text{stat})_2^2$; this is equivalent to $\kappa \rightarrow (\text{stat})_{\sigma}^2$ for all $\sigma < \kappa$, but is strictly weaker than $\kappa \rightarrow (\text{stat})_2^3$ (see BAUMGARTNER [1975]).

Obviously, κ being either ineffable or Ramsey implies that κ is weakly compact; but it also implies that the set of weakly compact cardinals below

* Appended by the editor and set-theory coordinator.

κ is a stationary subset of κ . The first Ramsey cardinal is not ineffable, but the ineffable cardinals are stationary below any Ramsey cardinal.

The existence of an ineffable cardinal does not refute Gödel's axiom of constructibility ($V = L$), but the existence of a Ramsey cardinal implies that $\mathcal{P}(\omega) \cap L$ is countable (see Section 6 of Chapter A.5, and SILVER [1973]). It also implies that every Σ_2^1 set of reals is Lebesgue measurable, whereas this statement is false in L (see Chapter C.8).

A still larger cardinal property, measurability, was motivated historically by the seemingly unrelated question of whether an ultrafilter can be countably complete. $\kappa > \omega$ is called measurable iff there is a κ -complete non-principal ultrafilter on κ . The existence of a measurable cardinal is equivalent to the existence of a countably complete non-principal ultrafilter on any set. If κ is measurable, κ is both Ramsey and ineffable, and the set of cardinals with both these properties is stationary below κ .

In Chapter A.3, there is a discussion of ultrapowers. Many of the results on measurable cardinals are proved by the method of Scott, which is to use the ultrafilter on κ to take an ultrapower of the whole universe of sets. The exposition of this given in SHOENFIELD [1971] cannot be improved upon.

Still larger cardinal axioms are obtained by postulating ultrafilters of specific types. For example, κ is *strongly compact* iff every κ -complete filter on any set can be extended to a κ -complete ultrafilter. SOLOVAY [1974] has shown that if κ is strongly compact, then the GCH holds at all singular strong limit cardinals above κ .

It is known (LÉVY and SOLOVAY [1967]) that the existence of a large cardinal cannot imply either CH or not CH. It is open whether cardinals like strongly compact or above imply anything interesting about descriptive set theory-like, e.g., measurability of Σ_3^1 sets of reals.

References

- BANACH, S. and TARSKI, A.
[1924] Sur la décomposition des ensembles de points en parties respectivement congruentes, *Fund. Math.*, **6**, 244–277.
- BARWISE, J.
[1975] *Admissible Sets and Structures* (Springer, Berlin).
- BAUMGARTNER, J.
[1975] *Ineffability properties of cardinals I*. Coll. Math. Soc. János Bolyai 10, Infinite and finite sets. Keszthely, 1973, pp. 109–130.
- DEVLIN, K. and JOHNSBRÄTEN, H.
[1974] *The Souslin Problem*, Lecture Notes in Mathematics, Vol. 405 (Springer, Berlin).
- DRAKE, F.
[1974] *Set Theory, an introduction to large cardinals* (North-Holland, Amsterdam).
- EASTON, W.
[1970] Powers of regular cardinals, *Ann. Math. Logic*, **1**, 139–178.

ERDŐS, P. and RADO, R.

[1952] Combinatorial theorems on classifications of subsets of a given set, *Proc. London Math. Soc.*, **2** (3), 417–439.

[1956] A partition calculus in set theory, *Bull. Am. Math. Soc.*, **62**, 427–489.

ERDŐS, P., HAJNAL, A. and RADO, R.

[1965] Partition relations for cardinal numbers, *Acta Math. Acad. Sci. Hungar.*, **16**, 93–196.

ERDOS, P., HAJNAL, A., MÁTÉ, A. and RADO, R.

[~ 1977] *Combinatorial Set Theory: Partition Relations for Cardinals*, to appear.

GALVIN, F. and HAJNAL, A.

[1975] Inequalities for cardinal powers, *Ann. of Math.*, **101**, 491–498.

HALMOS, P.

[1960] *Naive Set Theory* (Van Nostrand, New York).

JECH, T.

[1971] Trees, *J. Symbolic Logic*, **36**, 1–14.

JUHÁSZ, I.

[1971] *Cardinal Functions in Topology* (Mathematisch Centrum, Amsterdam).

KLEINBERG, E.

[1970] Strong partition properties for infinite cardinals, *J. Symbolic Logic*, **35**, 410–428.

KUNEN, K.

[1971] Elementary embeddings and infinitary combinatorics, *J. Symbolic Logic*, **36**, 407–413.

KUNEN, K.

[~ 1977] Saturated ideals, to appear.

LÉVY, A. and SOLOVAY, R.

[1967] Measurable cardinals and the continuum hypothesis, *Israel J. Math.*, **5**, 234–248.

LUZIN, N.

[1914] Sur un problème de M. Baire, *C.R. Acad. Sci. Paris*, **158**, 1258–1261.

MITCHELL, W.

[1972] Aronszajn trees and the independence of the transfer property, *Ann. Math. Logic*, **5**, 21–46.

RUDIN, M.E.

[1975] *Lectures on Set Theoretic Topology*, CBMS series, Vol. 23 (Am. Math. Soc., Providence, RI).

SHOENFIELD, J.

[1971] Measurable cardinals, in: *Logic Colloquium 69*, edited by R.D. Gandy and C.M.E. Yates (North-Holland, Amsterdam), pp. 19–49.

SIERPIŃSKI, W.

[1934] *Hypothèse du Continu* (Chelsea, New York; second edition, 1956).

SILVER, J.

[1973] The bearing of large cardinals on constructibility, in: *Studies in Model Theory*, MAA Studies in Mathematics, Vol. 8 (Math. Assoc. Am., Buffalo, NY), pp. 158–182.

SOLOVAY, R.

[1971] Real-valued measurable cardinals, in: *AMS Proceedings of Symposia in Pure Mathematics*, Vol. 13, part I (Am. Math. Soc., Providence, RI), pp. 397–428.

[1974] Strongly compact cardinals and the GCH, in: *AMS Proceedings of Symposia in Pure Mathematics*, Vol. 15 (Tarski Symposium) (Am. Math. Soc., Providence, RI), pp. 365–372.

SOLOVAY, R., REINHARDT, W. and KANAMORI, A.

[~ 1977] Strong axioms of infinity and elementary embeddings, to appear.

ULAM, S.

[1930] Zur Masstheorie in der allgemeinen Mengenlehre, *Fund. Math.*, **16**, 140–150.

B.4

Forcing

JOHN P. BURGESS

Contents

0. Introduction	404
Appendix. Some definitions	406
1. A closer look at models of set theory	408
2. Forcing	412
3. The Continuum Hypothesis	420
4. Useful combinatorial principles	428
5. Doing two things at once.	438
6. Martin's Axiom	444
References	451

Introduction

COHEN [1966] proved that adding the negation $\neg$ CH of the Continuum Hypothesis (CH) to the axioms of set theory does not lead to contradiction, unless the axioms themselves are already contradictory. In logicians' jargon, $\neg$ CH is *consistent relative to* the axioms of set theory. Since all classical mathematics follows from these axioms, and there is little chance of finding a contradiction in them, Cohen's work rules out a refutation of $\neg$ CH (a proof of CH, that is) by ordinary mathematical means. Since GÖDEL [1940] had earlier ruled out a disproof of CH (this is discussed in Chapter B.5 on constructibility), neither a positive nor a negative solution to the continuum problem can be given in classical mathematics.

Cohen's method, called forcing, has since been applied to prove (relative) consistency for hypotheses in transfinite arithmetic, infinitary combinatorics, general topology, measure theory, topology of the real line, universal algebra, and model theory. We hope to make the method accessible to readers innocent of logic and equipped with a minimum of set theory. (HALMOS [1960] suffices.) We will illustrate the method by proving consistency for some principles used elsewhere in this volume.

By "the" axioms of set theory we mean the Zermelo–Fraenkel axioms including Choice (ZFC). (See Chapter B.1. ZFC is essentially what Halmos uses.) Exact knowledge of the axioms is unnecessary. Trust that all classical mathematics following from them is necessary. The main definitions pertaining to cardinal and ordinal numbers are collected in an appendix to this section.

Non-Euclidean geometry was proved free from contradiction by exhibiting models for it. Likewise consistency proofs by forcing involve models. The definition of a *model* of ZFC requires some preliminaries.

0.1. Formal symbols for set theory

We introduce some formal symbolism for writing about sets:

Variables for sets $x, y, z, \dots$

Logical signs $\neg$ (not),

$\wedge$ (and), $\vee$ (or),

$\rightarrow$ (if ..., then ...), $\leftrightarrow$ (iff)

Quantifiers $\forall$ (for every), $\exists$ (there exists)

Identity sign $=$

Membership sign $\in$

plus parentheses for punctuation.

Examples. In this symbolism we express $y \subseteq x$ (y is a subset of x) thus:

$$(i) \quad \forall z (z \in y \rightarrow z \in x).$$

We can then express $w = \mathcal{P}(x)$ (the power set or set of all subsets of x) thus:

$$(ii) \quad \forall y (y \in w \leftrightarrow \forall z (z \in y \rightarrow z \in x)).$$

Finally the assertion that for all x , $\mathcal{P}(x)$ exists, is expressed thus:

$$(iii) \quad \forall x \exists w \forall y (y \in w \leftrightarrow \forall z (z \in y \rightarrow z \in x)).$$

This is one of the axioms of ZFC.

0.2. DEFINITION (Syntax). A sequence of formal symbols which corresponds to an English sentence, and not a mere phrase or jumble of words, is a (well-formed) *formula*. Thus 0.1(i)–(iii) are formulas, while the following are not:

$$\forall z (z \in y \rightarrow \text{ and } \vee \exists x) y = .$$

An occurrence of a variable x in a formula φ is *free* if it is not part of a clause of φ beginning with $\forall x$ or $\exists x$. Thus in 0.1(i), x, y are free. In 0.1(ii), x, w are free and y, z are not. 0.1(iii) has no free variables. Such formulas are called *closed formulas*, or sentences. (For more rigorous definitions, see Sections 2 and 3 of Ch. A.1.) Section 1 will provide more examples of translating English into formal symbolism. We hope readers will trust that even something like CH can be expressed by a closed formula.

0.3. DEFINITION (Semantics). A set a is *transitive* if whenever $b \in a$ and $c \in b$ we have $c \in a$; equivalently, if every element of a is a subset of a . If M is a transitive set, φ a closed formula, we say φ is true *inside* M , and write $M \models \varphi$, if φ comes out true when we read the quantifiers $\forall x, \exists x$ in φ as meaning not literally “for all sets x ” and “for some set x ” but rather “for all $x \in M$ ” and “for some $x \in M$ ”. If $\varphi(x_1 \cdots x_n)$ has free variables $x_1 \cdots x_n$ and $a_1 \cdots a_n \in M$, then $M \models \varphi(a_1 \cdots a_n)$ if φ comes out true when quantifiers are read as above and $x_1 \cdots x_n$ taken to stand for $a_1 \cdots a_n$ respectively.

Example. Let $\varphi(x, y)$ be the formula 0.1(i) expressing $y \subseteq x$. Then $M \models \varphi(a, b)$ iff for every $c \in M$, $c \in b$ implies $c \in a$. Since by transitivity M contains all $c \in b$, this amounts to saying all $c \in b$ have $c \in a$, i.e. $b \subseteq a$. In this case $M \models \varphi(a, b)$ iff $\varphi(a, b)$ is in fact true. Let $\psi(x, w)$ be

$\forall y (y \in w \leftrightarrow \varphi(x, y))$, which expresses that $w = \mathcal{P}(x)$. $M \models \psi(a, d)$ iff for all $b \in M$ we have: $b \in d$ iff $M \models \varphi(a, b)$, i.e. iff $b \subseteq a$. Since all $b \in d$ belong to M , this means all $b \in d$ are subsets of a , and all subsets of a which belong to M are in d , i.e. $d = \mathcal{P}(a) \cap M$. Since not all subsets of a need belong to M , we can have $M \models \psi(a, d)$ without $\psi(a, d)$ really being true, i.e. $d = \mathcal{P}(a) \cap M \neq \mathcal{P}(a)$. The power set axiom: $\forall x \exists w \psi(x, w)$ is true inside M if whenever $a \in M$, there is $b \in M$ with $M \models \psi(a, b)$; equivalently, if $a \in M$ implies $\mathcal{P}(a) \cap M \in M$.

A *model* of ZFC is a transitive set inside which all the axioms of ZFC are true. A countable, transitive model of ZFC is called a CTM. *We henceforth assume CTM's exist.* We show that this assumption implies the existence of a CTM M with $M \models \neg \text{CH}$. By any of several tricks known to logicians, a proof of this implication can be turned into a proof that if there is no contradiction in ZFC, then there is none in $\text{ZFC} + \neg \text{CH}$, the relative consistency result we mentioned at the beginning of this section. [Hint: apply the Compactness, Reflection, and Löwenheim–Skolem theorem, or see COHEN [1966] Chapter IV, Section 11.]

It may seem (to quote SKOLEM [1922]) “a peculiar and apparently paradoxical state of affairs” that ZFC, in which we can prove the existence of enormous uncountable sets, could have a countable model. After all, any element a of a CTM M will be a subset of M , and so like M will be countable. However (quoting Skolem again) “there is no contradiction at all if a set $a \dots$ is non-denumerable in the sense [of M]; for this only means that *within* M there is no one-to-one mapping Φ of a onto $\dots$ the [natural] number sequence”, which does not prevent such a Φ from existing *outside* M .

It is natural to abuse language by speaking of an English sentence being true inside a model when the corresponding formula is. In case we have two “translations” φ, ψ of the same English sentence, then if the translations are at all reasonable, the equivalence $\varphi \leftrightarrow \psi$ should be a theorem, and hence true inside any CTM M . Thus $M \models \varphi$ iff $M \models \psi$, and it does not matter which formula we think of as “the” official translation. We already used this abuse of language above in speaking of $a \in M$ being non-denumerable in the sense of M .

Appendix. Some definitions

See also Chapter B.1, and (for CUB sets and trees) Chapter B.3.

Ordinals may be characterized either as those transitive sets all of whose

elements are transitive, or as those transitive sets whose elements are linearly ordered by the $\in$ -relation. We reserve lower case Greek letters except $\varphi, \psi, \chi, \theta$ for ordinals. $\alpha < \beta$ iff $\alpha \in \beta$. Thus $\alpha = \{\beta : \beta < \alpha\}$. The *immediate successor* $\alpha + 1$ of α is $\alpha \cup \{\alpha\}$. An ordinal not 0 or an immediate successor of any other is called a *limit*. $\text{Lim}(\alpha)$ means that α is a limit. The least limit is called ω and its elements are the *finite* ordinals. The *supremum* of a set X of ordinals, $\sup X$, is the least ordinal $\geq$ every element of X . This is the same thing as $\bigcup X$, the set of all elements of elements of X . A *wellordering* of a set X is a linear ordering of X in which every nonempty subset of X has a least element. The $\in$ -relation provides a natural wellordering on any ordinal α . In fact any wellordering is isomorphic to the natural ordering on some unique ordinal, the (order) *type* of the wellordering.

The *cardinality* $\text{card } X$ of a set X is the least ordinal κ such that there exists a bijection between X and κ . A *cardinal* is an ordinal κ with $\text{card } \kappa = \kappa$. If κ is a cardinal, 2^κ or $\exp_2(\kappa)$ is $\text{card } \mathcal{P}(\kappa)$. κ^+ is the least cardinal $> \kappa$. ω_1 is ω^+ , ω_2 is ω_1^+ , etc. The Continuum Hypothesis (CH) is the proposition $2^\omega = \omega_1$. The Generalized Continuum Hypothesis (GCH) is the proposition that $2^\kappa = \kappa^+$ for all infinite cardinals κ . If α is a limit ordinal, its *cofinality* $\text{cf } \alpha$ is the least λ such that there is a function f with domain λ and $\sup \text{range } f = \alpha$. If κ is a cardinal, $\text{cf } \kappa$ is the least λ such that κ is the union of λ sets each of cardinality $< \kappa$. κ is *regular* if $\text{cf } \kappa = \kappa$, otherwise κ is *singular*. Cardinals of form κ^+ are *successor* cardinals, other cardinals are *limit* cardinals. κ is a *strong limit* if $2^\lambda < \kappa$ for all $\lambda < \kappa$. ω and all successor cardinals are regular. A regular strong limit cardinal is said to be (strongly) *inaccessible*.

Let α be a limit ordinal. $A \subseteq \alpha$ is *unbounded* in α if $\sup A = \alpha$. A is *closed* in α if whenever $\beta < \alpha$ and $\sup(A \cap \beta) = \beta$, then $\beta \in A$. A is CUB in α if A is both closed and unbounded in α . A is *stationary* in α if $A \cap C \neq \emptyset$ for every CUB $C \subseteq \alpha$. These notions trivialize when $\text{cf } \alpha = \omega$. If $\text{cf } \alpha > \omega$, then an intersection of $< \text{cf } \alpha$ CUB sets is CUB, the intersection of a stationary and a CUB set is stationary, etc. (See Section 2 of Chapter B.3.)

A relation $\leq$ *partially orders* a set X if $\leq$ is reflexive, transitive, and antisymmetric. A *tree* is a pair $T = \langle |T|, \leq_T \rangle$, where $\leq_T$ partially orders $|T|$, there is a $\leq_T$ least element, and for any $a \in |T|$, the set of $\leq_T$ -predecessors of a is wellordered by $\leq_T$. The type of this wellordering is the *rank* of a . The α -th *level* of T is $T_\alpha = \{a : \text{rank } a = \alpha\}$. The *height* of T is the least α with $T_\alpha = \emptyset$. A *branch* through T is a $B \subseteq |T|$ such that any two elements of B are $\leq_T$ -comparable, and B contains one element from

T_α for each $\alpha < \text{height } T$. We usually identify T and $|T|$. (See Section 4 of Chapter B.3.)

1. A closer look at models of set theory

We have seen that the formula $\varphi(x, y)$ expressing that $y \subseteq x$ enjoys the following property: If M is a CTM and $a, b \in M$, then $M \models \varphi(a, b)$ iff $\varphi(a, b)$ is in fact true. Such a formula we call *absolute*. A nonabsolute formula is the one $\psi(x, y)$ expressing that $y = \mathcal{P}(x)$. We say an English expression is absolute when the corresponding formula is.

1.1. LEMMA. *The following are absolute:*

- (i) $y = \bigcup x$, *the set of all elements of elements of x* ;
- (ii) $z = x \cap y$ (or $x \cup y$);
- (iii) $z = \{x, y\}$, *unordered pair*;
- (iv) $z = \langle x, y \rangle$, *ordered pair*;
- (v) $z = x \times y$, *Cartesian product*;
- (vi) z *is a function*;
- (vii) $(z \text{ is a binary relation}) \wedge x = \text{dom } z$, *the set of 1st components of elements of z (or $x = \text{range } z$, the set of 2nd components, or $x \subseteq \text{dom } z$, etc.)*;
- (viii) z *is an injection (or surjection, or bijection) from x to y* ;
- (ix) x *is transitive*;
- (x) $\text{OR}(x)$, x *is an ordinal*;
- (xi) $\text{Lim}(x)$, x *is a limit ordinal (or x is a successor, x is a finite ordinal, x is the ordinal ω)*;
- (xii) $\text{Lim}(x) \wedge y \subseteq x \wedge y$ *is unbounded (or closed, or CUB) in x* ;
- (xiii) y *is a reflexive (or transitive, antisymmetric, etc.) binary relation on x* .

PROOF. See Lemmas 1.3, 1.4 below. $\square$

1.2. DEFINITION. We write $\forall x \in y \varphi(x)$ and $\exists x \in y \varphi(x)$ to abbreviate $\forall x (x \in y \rightarrow \varphi(x))$ and $\exists x (x \in y \wedge \varphi(x))$. We write $\forall x \in z \varphi(x)$ and $\exists x \in z \varphi(x)$ to abbreviate $\forall y \in z \forall x \in y \varphi(x)$ and $\exists y \in z \exists x \in y \varphi(x)$. We call these new items of notation *bounded* quantifiers. A formula is Δ_0 if it can be so written, using these abbreviations, as to contain only bounded and no ordinary quantifiers.

The following result comes from LÉVY [1965], which contains much further information on absoluteness.

1.3. PROPOSITION. Δ_0 -formulas are absolute.

PROOF. In general “for every set x ” and “for every $x \in M$ ” are not equivalent, so truth inside a CTM M and genuine truth can diverge. But if $y \in M$, then “for every $x \in y$ ” and “for every $x \in M$ such that $x \in y$ ” amount to the same thing, since by transitivity all $x \in y$ belong to M . Since Δ_0 -formulas contain only bounded quantifiers like “for every $x \in y$ ”, for these formulas truth inside M and genuine truth coincide, i.e. they are absolute. $\square$

1.4. LEMMA. The notions of Lemma 1.1 can be expressed by Δ_0 -formulas.

PROOF. We exhibit the formulas (leaving items in parentheses in 1.1 to the reader).

- (i) $\forall w \in y \exists z \in x (w \in z) \wedge \forall w \in x (w \in y),$
- (ii) $\forall w \in z (w \in x \wedge w \in y) \wedge \forall w \in x (w \in y \rightarrow w \in z),$
- (iii) $x \in z \wedge y \in z \wedge \forall w \in z (w = x \vee w = y),$
- (iv) $\exists z_0 \in z \exists z_1 \in z (z = \{z_0, z_1\} \wedge z_0 = \{x, x\} \wedge z_1 = \{x, y\}),$
- (v) $\forall w \in z \exists x' \in x \exists y' \in y (w = \langle x', y' \rangle) \wedge$
 $\wedge \forall x' \in x \forall y' \in y \exists w \in z (w = \langle x', y' \rangle),$
- (vi) $\forall w \in z \exists x \in w \exists y \in w (w = \langle x, y \rangle) \wedge$
 $\wedge \forall w_0 \in z \forall w_1 \in z \forall x_0 \in w_0 \forall x_1 \in w_1 \forall y_0 \in w_0 \forall y_1 \in w_1$
 $(w_0 = \langle x_0, y_0 \rangle \wedge w_1 = \langle x_1, y_1 \rangle \wedge x_0 = x_1 \rightarrow y_0 = y_1),$
- (vii) $\forall w \in z \exists x' \in x \exists y \in w (w = \langle x', y \rangle) \wedge$
 $\wedge \forall x' \in x \exists w \in z \exists y \in w (w = \langle x', y \rangle),$
- (viii) $(z \text{ is a function}) \wedge x = \text{dom } z \wedge \text{range } z \subseteq y \wedge$
 $\wedge \forall w_0 \in z \forall w_1 \in z \forall x_0 \in x \forall x_1 \in x$
 $\forall y_0 \in y \forall y_1 \in y (w_0 = \langle x_0, y_0 \rangle \wedge w_1 = \langle x_1, y_1 \rangle \wedge$
 $\wedge y_0 = y_1 \rightarrow x_0 = x_1),$
- (ix) $\forall y \in x \forall z \in y (z \in x),$
- (x) $(x \text{ is transitive}) \wedge \forall y \in x (y \text{ is transitive}),$
- (xi) $\text{OR}(x) \wedge \forall z \in x \exists y \in x (z \in y),$

- (xii) $\text{Lim}(x) \wedge y \subseteq x \wedge \forall z \in x \exists w \in y (z \in w),$
- (xiii) $(y \text{ is a binary relation}) \wedge x = \text{dom } y \wedge x = \text{range } y \wedge$
 $\wedge \forall z \in x \exists w \in y (w = \langle z, z \rangle).$

It is understood that in (iv) “ $z = \{z_0, z_1\}$ ” is to be written out as a Δ_0 -formula using (iii). $\square$

1.5. Consequences of absoluteness

(i) We do not constantly have to be saying such things as, “Let $f \in M$ be such that $M \models f$ is a function”. It is enough to say, “Let $f \in M$ be a function”. By absoluteness of being a function, inside or outside M makes no difference.

(ii) Absoluteness guarantees that CTM’s are closed under many set-theoretic operations. If M is a CTM, $a \in M$ a binary relation, then it is a theorem (of naive set theory, and of ZFC) that we can form the set $\text{range } a$ of 2nd components of elements of a . This being true inside M , there must be $b \in M$ such that $M \models (b = \text{range } a)$. By absoluteness of ranges, this b can only be the genuine range of a , so $\text{range } a \in M$, and M is closed under taking ranges.

Similarly, M is closed under forming pairs, under $\cap$ and $\times$, etc. Also ω and all finite ordinals belong to M . From 1.6 below it will follow M is closed under the operation $\mathcal{P}_\omega(a) = \{b \subseteq a : b \text{ is finite}\}$.

(iii) Zermelo’s Separation Axiom, an important axiom of ZFC, says that for any set a and formula $\varphi(x)$ we can form $\{b \in a : \varphi(b)\}$. Applied to a CTM M this means that for $a \in M$ we can form $\{b \in a : M \models \varphi(b)\}$ inside M . In case φ is absolute, this equals $\{b \in a : \varphi(b)\}$. Thus we can “separate” the ordinals, or functions, etc. from $a \in M$ forming $\{b \in a : \text{OR}(b)\}$, $\{f \in a : f \text{ is a function}\}$ in M .

(iv) We can combine closure properties of a CTM M to get new ones. Thus if $a_1 \cdots a_n \in M$, then by closure under singletons and union, we see $\{a_1 \cdots a_n\} \in M$. Thus M is closed under forming finite subsets.

Combining closure under $\cap$, $\times$, range, and $\mathcal{P}_\omega$, and separating ordinals and functions, we see that the following belong to M if a, b do:

$$\{c \in \text{range } a : \exists d \in b (\langle d, c \rangle \in a)\} = \text{range}(a \cap (b \times \text{range } a)),$$

$$\{b \in \text{range } a : \text{OR}(b)\},$$

$$\begin{aligned} \{f : (f \text{ is a function}) \wedge (\text{dom } f \text{ is finite}) \wedge \text{dom } f \subseteq a \wedge \text{range } f \subseteq b\} = \\ = \{f \in \mathcal{P}_\omega(a \times b) : f \text{ is a function}\}. \end{aligned}$$

Below when working with a CTM M we frequently assert that various sets belong to M . These claims can be justified by the method just illustrated (though sometimes it is necessary to check that some notion not on the list 1.1 is absolute). On first reading it may be well just to trust us on these claims so as not to lose the thread of our arguments.

(v) By absoluteness, for any CTM M and any $a \in M$, we have $M \models \text{OR}(a)$ iff a is in fact an ordinal. Let OR^M be the least ordinal $\alpha \notin M$. Then if $\beta \in M$, $\gamma < \beta$ (i.e. $\gamma \in \beta$), then $\gamma \in M$. Thus $\{\beta \in M: \text{OR}(\beta)\} = \{\beta: \beta < \text{OR}^M\} = \text{OR}^M$.

(vi) Some nonabsolute notions: For a CTM M and $a \in M$, write $\mathcal{P}^M(a)$ for the power set of a in the sense of M , i.e. the $b \in M$ such that $M \models (b = \mathcal{P}(a))$. Using the absoluteness of the subset relation, we saw in 0.3 above that $\mathcal{P}^M(a) = \mathcal{P}(a) \cap M$. Similarly, write $\text{card}^M a$ for the $b \in M$ such that $M \models (b = \text{card } a)$. The absoluteness of being an ordinal or a bijection then tell us that $\text{card}^M a$ is the least ordinal $\alpha < \text{OR}^M$ such that there is a bijection between a and α which belongs to M . If $a \in \mathcal{P}^M(\alpha)$ for some $\alpha < \text{OR}^M$, then the absoluteness of CUB shows that $M \models (a \text{ is stationary in } \alpha)$ iff $a \cap C \neq \emptyset$ for every CUB $C \subseteq \alpha$ which belongs to M . Power set, cardinality, stationary subset are not themselves absolute notions, but absoluteness of some related notions has enabled us to see what these notions do amount to inside a CTM.

Intuitively a property is absolute if we can check whether it holds for elements of a CTM M without leaving M . Thus to check for $a, b, c \in M$ whether $c = \{a, b\}$, we need to check that $a, b \in c$ and that c has no elements other than a, b . Since all elements of c belong to M , we do not need to leave M to do this. By contrast, to check for $\alpha < \text{OR}^M$ and $a \subseteq \alpha$ whether a is a stationary subset of α requires checking whether $a \cap C \neq \emptyset$ for all CUB $C \subseteq \alpha$. Since not all such C belong to M , we are unable to check this inside M .

1.6. LEMMA. *The following are absolute:*

- (i) x is finite,
- (ii) $y = \mathcal{P}_\omega(x)$,
- (iii) y is a wellordering of x ,
- (iv) $(y \text{ is a wellordering of } x) \wedge \text{OR}(z) \wedge (z \text{ is the order type of } y)$.

PROOF. It is known that these items cannot be expressed by Δ_0 -formulas, so we must use instead our intuitive understanding of the meaning of absoluteness. We give the proof for (i), leaving (ii) to the reader. (iii) requires more difficult arguments and its proof will be omitted. (See LÉVY

[1965].) (iv) follows using (iii) and the absoluteness of being an isomorphism between orderings (a slight extension of the absoluteness of being a bijection).

Let M be a CTM, $a \in M$. To check whether a is finite, we need to know whether there is a bijection from a finite ordinal onto a . Being a finite ordinal and being a bijection are absolute. Moreover all finite ordinals belong to M . Thus to prove absoluteness it suffices to show that if there does exist a bijection f between a and a finite ordinal n , then this f belongs to M . But f is a finite set of ordered pairs of elements of M , and M is closed under pairing and finite subsets, so $f \in M$ as required. $\square$

Armed with the information on CTM's provided by this section, we can turn to a study of the forcing method for constructing CTM's with special properties.

2. Forcing

The methods of COHEN [1966] have been enormously streamlined and generalized through the work of many set-theorists (not including the present writer). Since many were involved, we attach no individual names to the basic lemmas in this section and the next. We do credit particular consistency results obtained by the forcing method to their authors. Our account of forcing derives from SHOENFIELD [1971] and from lectures of Solovay, among the foremost contributors to the theory of forcing.

2.1. DEFINITION. A PO set is a pair $P = \langle |P|, \leq_P \rangle$, where

(i) $\leq_P$ partially orders $|P|$ (i.e. is a reflexive, transitive, antisymmetric relation on $|P|$),

(ii) there exists a $\leq_P$ -greatest element 1_P ,

(iii) there exist no $\leq_P$ -minimal elements. We usually identify the structure P and the *underlying set* $|P|$, and drop subscripts from $\leq$ and 1 .

If P is a PO set and $p, q \in P$, we say:

$p < q$ iff $p \leq q$ and not $q \leq p$,

p, q are *comparable* iff $p \leq q$ or $q \leq p$,

p, q are *compatible* iff there exists r with $r \leq p$ and $r \leq q$,

p, q are *incompatible* iff no such r exists.

If P is a PO set and $A \subseteq P$, we say:

A is *open* iff whenever $p \in A$ and $q \geq p$, then $q \in A$,

A is *dense* iff for every $p \in P$ there is $q \in A$ with $q \leq p$,

A is an *antichain* iff any two distinct elements of A are incompatible.

Note that an antichain $A \subseteq P$ is *maximal* iff every $p \in P$ is compatible with some $q \in A$. We say $A \subseteq P$ is *dense below* $p \in P$ iff for every $p' \leq p$ there is $q \in A$ with $q \leq p'$. *Antichains below* p are similarly defined.

If P, Q are PO sets, we say Q is a *suborder* of P if $|Q| \subseteq |P|$, $1_P \in |Q|$ and $\leq_Q$ is just the restriction of $\leq_P$ to $|Q|$. If $\text{Lim}(\lambda)$ and P_α , $\alpha < \lambda$, are PO sets, we say the sequence of P_α 's is *increasing* if P_α is a suborder of P_β for $\alpha < \beta$. The *union* of such an increasing sequence is the PO set P_λ whose underlying set is the union of the underlying sets of the P_α 's and whose (partial) order relation is the union of the order relations of the P_α 's. These notions will become important in Section 5.

2.2. DEFINITION. Let P be a PO set, F any family of sets, $G \subseteq P$. Then G is *F-generic* iff the following hold:

- (i) Whenever $p \in G$ and $p \leq q$, then $q \in G$.
- (ii) Whenever $p, q \in G$, then there exists $r \in G$ with $r \leq p$ and $r \leq q$. In particular, any two elements of G are compatible.
- (iii) $G \cap D \neq \emptyset$ for any dense $D \subseteq P$ with $D \in F$.

2.3. PROPOSITION. Let P be a PO set, F a family of sets containing only countable many dense subsets of P , and $p \in P$. Then there exists an *F-generic* $G \subseteq P$ with $p \in G$.

PROOF. Enumerate the dense subsets of P in F as $\{D_n : n \in \omega\}$. We pick elements p_n of P as follows: Let $p_0 = p$. If p_n is defined, pick $p_{n+1} \leq p_n$ with $p_{n+1} \in D_n$. This is possible since D_n is dense. Let $G = \{q \in P : \exists n \in \omega (p_n \leq q)\}$. Clearly $p \in G$ and 2.2(i), (iii) hold. Now (ii) also holds. For if $q, r \in G$, say $p_m \leq q$, $p_n \leq r$, then p_k is $\leq$ both q and r , where $k = \max(m, n)$. $\square$

Let M be a CTM, $P \in M$ a PO set. Taking $F = M$ in 2.3, we see for any $p \in P$ there exists an M -generic $G \subseteq P$ with $p \in G$. For most P it can be shown that *no such G belongs to M* .

2.4. DEFINITION. Let P be a PO set. Any subset of a set of form $P \times a$ is called a *P-term*. If $t \subseteq P \times a$ is a *P-term* and $G \subseteq P$, the *G-interpretation* of t , $I_G(t)$ is defined to be $\{b \in a : \exists p \in G ((p, b) \in t)\}$.

Examples. For any a , let $a^* = P \times a$. Then for any nonempty G , $I_G(a^*) = a$. Let $\bar{G} = \{\langle p, p \rangle : p \in P\}$. Then for any G , $I_G(\bar{G}) = G$.

For proofs of the following lemma, and of Lemmas 2.9 and 2.11, we refer the reader to SHOENFIELD [1971]. It is hardly surprising that in a short exposition we should have to assume some results without proof. What is rather surprising is that these three lemmas imply everything we will need to know about forcing.

2.5. EXISTENCE AND MINIMALITY LEMMA. *Let M be a CTM, $P \in M$ a PO set, and $G \subseteq P$ M -generic. Then there exists a smallest CTM N with the properties that $M \subseteq N$ and $G \in N$. Moreover, if $a \subseteq M$ and $a \in N$, then $a = I_G(t)$ for some P -term $t \in M$.*

We write $N = M[G]$ and call N the *Cohen extension* obtained by adjoining G to the ground model M .

(Notice that since $G \notin M$, N is a proper extension of M . Notice also that by remarks in 1.5(iv), any CTM N with $t, G \in N$ will have $I_G(t) \in N$. Thus $a \subseteq M$ is in $M[G]$ iff a has form $I_G(t)$ for some $t \in M$.)

2.6. PROPOSITION. *Let M be a CTM, $P \in M$ a PO set, $G \subseteq P$ M -generic, $M = M[G]$. Then $\text{OR}^N = \text{OR}^M$.*

PROOF. Recall $\text{OR}^M = \{\alpha \in M : \text{OR}(\alpha)\}$ = the least ordinal $\alpha \notin M$. So it suffices to show $\text{OR}^M \notin N$. Suppose the contrary. Then $\text{OR}^M = I_G(t)$ for some $t \in M$. By our remarks in 1.5(iv), whenever $a \in M$, $\{\alpha \in \text{range } a : \text{OR}(\alpha)\} \in M$. Hence $\text{OR}^M = \{\alpha \in \text{range } t : \text{OR}(\alpha)\} \in M$, a contradiction. $\square$

2.7. DEFINITION. Let M be a CTM, $P \in M$ a PO set, $p \in P$, $t_1 \cdots t_n \in M$ P -terms, and $\varphi(x_1 \cdots x_n)$ a formula with free variables $x_1 \cdots x_n$. We say p *P -forces $\varphi(t_1 \cdots t_n)$ over M* , and write

$$p \Vdash_M^P \varphi(t_1 \cdots t_n)$$

if $M[G] \models \varphi(I_G(t_1) \cdots I_G(t_n))$ for every M -generic $G \subseteq P$ with $p \in G$. We generally omit the sub- and superscripts on $\Vdash$.

Example. If $p \leq q$, and $q^*, \bar{G}$ are the terms defined in 2.4 above, then $p \Vdash q^* \in \bar{G}$. For if $G \subseteq P$ is M -generic and $p \in G$, then $q = I_G(q^*) \in G = I_G(\bar{G})$. If instead p, q are incompatible, then $p \Vdash q^* \notin \bar{G}$, since $p \in G$ implies $q \notin G$ for generic G .

We speak of an English expression being forced when the corresponding formula is. Intuitively, something is forced by p if we can tell it is going to be

true in $M[G]$ just by knowing that $p \in G$. Since an element p of P thus restricts the possibilities as to what may happen in $M[G]$, the elements of P are often called *conditions*. When $p \leq q$, p is more restrictive than q ($p \in G$ implies $q \in G$ for generic G), so p is said to be a *stronger* condition.

2.8. PROPOSITION. *Let M be a CTM, $P \in M$ a PO set, $p \in P$, $a \in M$, φ , etc. formulas. Then the following hold:*

(i) *If $p \Vdash \varphi_1 \cdots p \Vdash \varphi_n$, and if $\varphi_1 \cdots \varphi_n$ together with the axioms of ZFC logically imply φ , then $p \Vdash \varphi$.*

(ii) *Not both $p \Vdash \varphi$ and $p \Vdash \neg \varphi$.*

(iii) *If $p \Vdash \varphi$ and $q \leq p$, then $q \Vdash \varphi$.*

(iv) *If $p \Vdash \varphi$ and $q \Vdash \neg \varphi$, then p, q are incompatible.*

(v) *$p \Vdash \varphi \wedge \psi$ iff both $p \Vdash \varphi$ and $p \Vdash \psi$.*

(vi) *$p \Vdash \forall x \in a^* \theta(x)$ iff for all $b \in a$, $p \Vdash \theta(b^*)$.*

(vii) *$p \Vdash \forall x (x \subseteq a^* \rightarrow \theta(x))$ iff for all $t \in \mathcal{P}^M(a^*)$, $p \Vdash \theta(t)$.*

PROOF. These are pleasant exercises in the definitions, and readers may wish to try them before reading the hints that follow:

(i) For any M -generic $G \subseteq P$ with $p \in G$, $\varphi_1 \cdots \varphi_n$ and all the axioms of ZFC are true inside $M[G]$, hence so is φ .

(ii) By 2.3 there exists a generic G with $p \in G$. Not both $M[G] \models \varphi$ and $M[G] \models \neg \varphi$.

(iii) When $q \leq p$, any generic G with $q \in G$ also has $p \in G$.

(iv) Follows from (ii) and (iii).

(v) The RHS of (v) means that first for any generic G with $p \in G$, $M[G] \models \varphi$, and second that any such $M[G] \models \psi$. The LHS means that for any such G , $M[G] \models \varphi \wedge \psi$ — which is the same thing!

(vi) For any generic G , any element of $I_G(a^*) = a$ has form $I_G(b^*) = b$ for some $b \in a$. This noted, (vi) becomes, like (v), a tautology.

(vii) For any generic G , any subset of a in $M[G]$ has form $I_G(t)$ for some $t \in M$. It is no real restriction to consider only $t \subseteq a^*$, since in general $I_G(t \cap a^*) = I_G(t) \cap a$. This noted, (vii) is a tautology. $\square$

In order to determine when $p \Vdash \neg \varphi$, we need a deeper result. (See SHOENFIELD [1971].) Note the “if” part of the following is part of Definition 2.7.

2.9. TRUTH LEMMA. *Let M be a CTM, $P \in M$ a PO set, $G \subseteq P$ M -generic, $t_1 \cdots t_n \in M$ P -terms, and $\varphi(x_1 \cdots x_n)$ a formula. Then $M[G] \models \varphi(I_G(t_1) \cdots I_G(t_n))$ iff there is a $p \in G$ such that $p \Vdash_M^P \varphi(t_1 \cdots t_n)$.*

2.10. PROPOSITION. *Let the notation be as in 2.8. Then:*

- (i) $p \Vdash \neg \varphi$ iff no $q \leq p$ has $q \Vdash \varphi$.
- (ii) If $\{r \in P: r \Vdash \varphi\}$ is dense below p in P , then $p \Vdash \varphi$.
- (iii) $p \Vdash \varphi \vee \psi$ iff for every $q \leq p$ there exists $r \leq q$ such that either $r \Vdash \varphi$ or $r \Vdash \psi$.
- (iv) $p \Vdash \exists x \in a^* \theta(x)$ iff for every $q \leq p$ there exist $r \leq q$ and $b \in a$ such that $r \Vdash \theta(b^*)$.
- (v) $p \Vdash \exists x (x \subseteq a^* \wedge \theta(x))$ iff for every $q \leq p$ there exist $r \leq q$ and $t \in P^M(a^*)$ such that $r \Vdash \theta(t)$.

PROOF. (i) The “only if” part follows from 2.8(iv). For the “if” part, suppose we do not have $p \Vdash \neg \varphi$. Then there is a generic G with $p \in G$ and $M[G] \models \varphi$. By the Truth Lemma, there is $q \in G$ with $q \Vdash \varphi$. We may suppose $q \leq p$. If not, there is $q' \in G$ with $q' \leq p$, $q' \leq q$. By 2.8(iii) this q' still forces φ . Thus if not $p \Vdash \neg \varphi$, there is $q \leq p$ with $q \Vdash \varphi$. Contraposing gives (i).

(ii) If $\{r \in P: r \Vdash \varphi\}$ is dense below p , then by 2.8(iv), no $q \leq p$ can force $\neg \varphi$. By (i), $p \Vdash \neg \neg \varphi$, and by 2.8(i), $p \Vdash \varphi$.

(iii), (iv), (v) follow from (i), 2.8(v), (vi), (vii), and the equivalence of $\varphi \vee \psi$ to $\neg(\neg \varphi \wedge \neg \psi)$ and $\exists x \theta(x)$ to $\neg \forall x \neg \theta(x)$. $\square$

2.11. DEFINABILITY LEMMA. *To every formula $\varphi(x_1 \cdots x_n)$ we can associate a formula $\varphi^*(x_1 \cdots x_n, y, z)$ such that for any CTM M , any PO set $P \in M$, any $p \in P$, and any P -terms $t_1 \cdots t_n \in M$ we have:*

$$p \Vdash_M^P (t_1 \cdots t_n) \quad \text{iff} \quad M \models \varphi^*(t_1 \cdots t_n, p, P).$$

For a proof we refer the reader again to SHOENFIELD [1971]. Note that our definition of forcing (2.7) does *not* directly provide us with suitable formulas φ^* . The definition of forcing in terms of M -generic sets is something we can *not* talk about inside M ; inside M there just *aren't* any M -generic sets. In fact φ^* must be obtained quite deviously and is quite complicated even for simple φ like $(x_1 \in x_2)$.

An important consequence of 2.11 is the following closure property: If M is a CTM, $P \in M$ a PO set, $T_1 \cdots T_n \in M$ sets of P -terms, $\varphi(x_1 \cdots x_n)$ a formula, and

$$E = \{\langle p, t_1 \cdots t_n \rangle \in P \times T_1 \times \cdots \times T_n: p \Vdash \varphi(t_1 \cdots t_n)\},$$

then $E \in M$. This follows from Zermelo's Separation Axiom (cf. 1.5(iii)) since $E = \{\langle p, t_1 \cdots t_n \rangle: M \models \varphi^*(t_1 \cdots t_n, p, P)\}$.

By abuse of language we will write, e.g. $M \models (p \Vdash^P t \text{ is a cardinal})$ when

we mean $M \models \varphi^*(t, p, P)$, where $\varphi(x)$ expresses that x is a cardinal — in other words, when we mean that $p \Vdash_M^P t$ is a cardinal. All such talk of forcing inside a CTM M involves implicit appeal to the Definability Lemma.

It will be useful to know that the notions introduced in Definitions 2.1 and 2.2 are absolute.

2.12. LEMMA. *The following are absolute:*

- (i) x is a PO set.
- (ii) $(x \text{ is a PO set}) \wedge y, z \in |x| \wedge y \leq_x z$ (or $y < z$; or y, z are comparable, or compatible, or incompatible).
- (iii) $(x \text{ is a PO set}) \wedge y \subseteq |x| \wedge y$ is open (or dense, or an antichain, or a maximal antichain, or dense below $x' \in |x|$, etc.).
- (iv) $(x \text{ is a PO set}) \wedge (y \text{ is a family of sets}) \wedge z \subseteq |x| \wedge z$ is y -generic.
- (v) $(x \text{ is a PO set}) \wedge y \subseteq |x| \wedge z \in |x| \wedge \exists z' \in y (z \leq_x z')$.

PROOF. We can express each of these by a Δ_0 -formula. E.g. (i) becomes:

$$\begin{aligned} & \exists x_0 \in x \exists x_1 \in x (x = \langle x_0, x_1 \rangle \\ & \wedge (x_1 \text{ is a reflexive, transitive, antisymmetric binary relation on } x_0) \\ & \wedge \exists y \in x_0 \forall y' \in x_0 \exists z \in x_1 (z = \langle y', y \rangle) \\ & \wedge \forall y \in x_0 \exists y' \in x_0 (\exists z \in x_1 (z = \langle y', y \rangle) \\ & \wedge \neg \exists z \in x_1 (z = \langle y, y' \rangle))). \end{aligned}$$

Here reflexivity, etc. are to be expressed as Δ_0 -formulas by Lemma 1.4. Alternatively, we could work with our intuitive understanding of absoluteness and show that for a CTM M and $P \in M$, we can check whether P is a PO set without leaving M . This is in fact not hard to see, since having all the elements of P available to us inside M , we can easily check for the existence of a maximum and the nonexistence of minimal elements.

We leave verification of absoluteness for (ii)–(v) to the reader. $\square$

Our remarks 1.5 on consequences of absoluteness apply also to these notions. Thus we don't have to say, "Let $P \in M$ be such that $M \models (P \text{ is a PO set})$ ". We can just say, "Let $P \in M$ be a PO set". Thus also given a CTM M , a PO set $P \in M$, and $A \in \mathcal{P}^M(P)$, we can form $D = \{q \in P : \exists p \in A (q \leq p)\}$ inside M , since this just involves "separating" the elements of P satisfying a certain condition which 2.12(v) tells us is absolute. Below we will frequently claim that certain sets whose definitions

involve notions pertaining to PO sets can be formed inside a CTM. On first reading it may be best just to trust us, but these claims *can* all be justified by showing some formula to be absolute. We give one example in the next lemma.

2.13. LEMMA. *Let M be a CTM, $P \in M$ a PO set, $p \in P$, $G \subseteq P$ an M -generic set with $p \in G$. Then $G \cap D \neq \emptyset$ for any $D \in \mathcal{P}^M(P)$ which is dense below p .*

PROOF. Let $E = \{q \in P: q \in D \vee q, p \text{ are incompatible}\}$. This set can be formed inside M since its definition is absolute (cf. 2.12(ii)). Any $q \in P$ which is not incompatible with p has an $r \leq q$ with $r \leq p$, and hence by density of D below p , an $s \leq r \leq q$ with $s \in D$. This shows E is fully dense in P , so by M -genericity, $G \cap E \neq \emptyset$. But since $p \in G$, no element of G is incompatible with p , so $G \cap D \neq \emptyset$ as required. $\square$

The following strengthening of 2.10(v) will not be used until Section 6, and can be skipped on first reading. Its proof is a *tour de force*.

2.14. THEOREM. *Let the notation be as in 2.8 and 2.10. Then $p \Vdash \exists x (x \subseteq a^* \wedge \theta(x))$ iff there exists $t \in \mathcal{P}^M(a^*)$ such that $p \Vdash \theta(t)$.*

PROOF. The “if” part is immediate. We break the proof of the “only if” part into a series of lemmas.

2.15. LEMMA. *Let M be a CTM, $P \in M$ a PO set, $p \in P$, $A \in \mathcal{P}^M(P)$ a maximal antichain below p . Then:*

- (i) *For any M -generic $G \subseteq P$ with $p \in G$, there is a unique $q \in A \cap G$.*
- (ii) *For any formula φ , if $q \Vdash \varphi$ for all $q \in A$, then $p \Vdash \varphi$.*

PROOF. (i) Let G be generic, $p \in G$. Since elements of generic sets are compatible, $A \cap G$ contains *at most* one element. Let $D = \{r \in P: \exists q \in A (r \leq q)\}$. We remarked (following 2.12) that this set can be formed inside M . We claim D is dense below p .

For let $p' \leq p$ be arbitrary. By maximality of A , there is $q \in A$ compatible with p' . Hence there is $r \leq p'$ with $r \leq q \in A$, whence $r \in D$. This proves density.

By 2.13, $D \cap G \neq \emptyset$. If $r \in D \cap G$, there is $q \in A$ with $r \leq q$, whence $q \in G$. Thus $A \cap G \neq \emptyset$ as required.

- (ii) Suppose $q \Vdash \varphi$ for all $q \in A$. Let G be generic with $p \in G$. By (i),

$A \cap G \neq \emptyset$, and there is $q \in G$ forcing φ . Thus $M[G] \models \varphi$, as required to show $p \Vdash \varphi$. $\square$

2.16. LEMMA. *Let M be a CTM, $P \in M$ a PO set. Then:*

(i) *If $A \in \mathcal{P}^M(P)$ is a maximal antichain, and $F \in M$ a function with $\text{dom } F = A$ and $F(q)$ a P -term for every $q \in A$, then there is a single P -term t such that $q \Vdash t = F(q)$ for every $q \in A$.*

(ii) *If $p \in P$ and $t, u \in M$ are P -terms, then there is a P -term $v \in M$ such that $p \Vdash v = t$ and any q incompatible with p has $q \Vdash v = u$.*

PROOF. (i) Since $A, F \in M$, we can form inside M $a = \bigcup \{\text{range } F(q) : q \in A\}$, a single set with $F(q) \subseteq P \times a$ for all $q \in A$. We can also form

$$t = \{\langle r, b \rangle \in P \times a : \exists q \in A \exists p \in P (r \leq q \wedge r \leq p \wedge \langle p, b \rangle \in F(q))\}.$$

It suffices to check that for generic G and $q \in A \cap G$, $I_G(t) = I_G(F(q))$.

Suppose first $b \in I_G(F(q))$. Then $\langle p, b \rangle \in F(q)$ for some $p \in G$. Take $r \in G$ with $r \leq q$ and $r \leq p$. By construction $\langle r, b \rangle \in t$, so $b \in I_G(t)$. Conversely, suppose $b \in I_G(t)$, i.e. there is $r \in G$ with $\langle r, b \rangle \in t$. By construction there are $q' \in A$ and p such that $r \leq q'$, $r \leq p$, and $\langle p, b \rangle \in F(q')$. Since $r \leq q'$, $q' \in G$. Since $A \cap G$ contains just one element, $q' = q$ and $\langle p, b \rangle \in F(q)$. Since $r \leq p$, $p \in G$, and finally $b \in I_G(F(q))$ as required.

(ii) Since Zorn's Lemma is true inside M (and since being a maximal antichain is absolute, cf. 2.12(iii)), there must be a maximal antichain $A \in M$ with $p \in A$. Let $F \in M$ be the function with $\text{dom } F = A$, $F(p) = t$, and $F(q) = u$ for all other $q \in A$. Applying (i) to this F we get a term v with $p \Vdash v = t$ and $q \Vdash v = u$ for any other $q \in A$. Now if q is anything incompatible with p , $A - \{p\}$ is a maximal antichain below q , so by 2.15(ii), $q \Vdash v = u$ as required. $\square$

Proof of the "only if" part of 2.14 modulo 2.15 and 2.16:

With notation as in 2.8 and 2.10, we have $p \Vdash \exists x (x \subseteq a^* \wedge \theta(x))$. Applying Zorn's Lemma inside M (and absoluteness considerations), there is an $F \in M$ maximal with respect to the property:

$$(F \text{ is a function}) \wedge (\text{dom } F \text{ is an antichain below } p) \wedge \\ \wedge q \Vdash \theta(F(q)) \text{ for all } q \in \text{dom } F.$$

(Recall that the set $E = \{\langle q, t \rangle \in P \times \mathcal{P}^M(a^*) : q \Vdash \theta(t)\}$ belongs to M as a consequence of the Definability Lemma. The last condition in the definition of F just says that $F \subseteq E$.)

We claim $\text{dom } F$ is a *maximal* antichain below p . For assume for contradiction that $p' \leq p$ is incompatible with all $q \in \text{dom } F$. Since $p' \Vdash \exists x (x \subseteq a^* \wedge \theta(x))$, by 2.10(v) there are $p'' \leq p'$ and $t \in P^M(a^*)$ such that $p'' \Vdash \theta(t)$. A fortiori p'' is incompatible with every $q \in A$. So $F \cup \{\langle p'', t \rangle\}$ is a counterexample to maximality of F , a contradiction.

Now apply 2.16(i) to this F to obtain a term t with $q \Vdash t = F(q)$ for all $q \in \text{dom } F$. Since $q \Vdash \theta(F(q))$ for all such q , $q \Vdash \theta(t)$. By 2.15(ii), $p \Vdash \theta(t)$. $\square$

2.17. COROLLARY. *Let notation be as in 2.8, 2.10, and 2.14. Suppose $1_P \Vdash \exists x (x \subseteq a^* \wedge \theta(x))$, and $t \in P^M(a^*)$, and $p \Vdash \theta(t)$. Then there is $v \in P^M(a^*)$ such that $1_P \Vdash \theta(v)$ and $p \Vdash v = t$.*

PROOF. Note that in general $1_P \Vdash \varphi$ iff every $q \in P$ forces φ . By 2.14 there is u with $1_P \Vdash \theta(u)$. Let $A \in M$ be a maximal antichain with $p \in A$. Using 2.15(i) we get a v with $p \Vdash v = t$ and $q \Vdash v = u$ for every other $q \in A$. Thus all $q \in A$ force $\theta(v)$, so $1_P \Vdash \theta(v)$ by 2.15(i). $\square$

It is often convenient to write $P \Vdash \varphi$ for $1_P \Vdash \varphi$.

3. The Continuum Hypothesis

What does it mean for the Continuum Hypothesis (CH) to be false, i.e. for $\neg \text{CH}$ to be true, inside a CTM M ? If κ is a cardinal in M , i.e. if $M \models (\kappa \text{ is a cardinal})$, let us write $(2^\kappa)^M$ or $\exp 2^M(\kappa)$ for $\text{card}^M(\mathcal{P}^M(\kappa))$. We also write $(\kappa^+)^M$ for the $\lambda \in M$ such that $M \models (\lambda \text{ is the least cardinal } > \kappa)$, and ω_1^M for $(\omega^+)^M$, ω_2^M for $(\omega_1^M)^+$, etc. Now CH is false iff there is an injection from ω_2 into $\mathcal{P}(\omega)$, or equivalently if there is a function $g : \omega_2 \times \omega \rightarrow \{0, 1\}$ such that:

- (*) Whenever $\alpha \neq \beta$ and $\langle \alpha, 0 \rangle$ and $\langle \beta, 0 \rangle \in \text{dom } g$,
then there exists $n \in \omega$ such that $g(\alpha, n) \neq g(\beta, n)$.

(Such a g gives rise to an injection $f(\alpha) = \{n \in \omega : g(\alpha, n) = 0\}$.) Thus $M \models \neg \text{CH}$ iff there is an injection $f \in M$ from ω_2^M to $\mathcal{P}^M(\omega)$. (Recall that being an injection is absolute.) Equivalently, $M \models \neg \text{CH}$ iff there is a map $g \in M$ from $\omega_2^M \times \omega$ to $\{0, 1\}$ satisfying (*).

If we start with an arbitrary CTM M (we are assuming one exists), we may have such a $g \in M$ (i.e. $M \models \neg \text{CH}$) and we may not. COHEN [1966]

shows how to construct an extension N of M in which such a g does exist for certain.

3.1. DEFINITION. Let α be an ordinal. Consider

$$P = \{p: (p \text{ is a function}) \wedge (\text{dom } p \text{ is finite})$$

$$\wedge \text{dom } p \subseteq \alpha \times \omega \wedge \text{range } p \subseteq \{0, 1\}.$$

Partially order P by *reverse inclusion*: $p \leq q$ iff $q \subseteq p$, i.e. if p is a function extending q . This makes P a PO set. The maximum element 1_P is the empty function. There are no minimal elements since every function in P has a proper extension in P . We call this P the α -Cohen PO set. Note that if M is a CTM and $\alpha < \text{OR}^M$, then by remarks in 1.5(iv), the α -Cohen PO set can be formed inside M . Elements of the α -Cohen PO set are in an obvious sense "finite approximations" to a function $\alpha \times \omega \rightarrow \{0, 1\}$.

3.2. LEMMA. Let M be a CTM, P the ω_2^M -Cohen PO set, $G \subseteq P$ M -generic, $N = M[G]$, and $g \in N$ the union $\bigcup G$ of all functions $p \in G$. Then:

- (i) g is a function.
- (ii) $\text{dom } g = \omega_2^M \times \omega$.
- (iii) g satisfies (*) above.

PROOF. (i) Clearly $g \subseteq \omega_2^M \times \omega \times \{0, 1\}$. If g were not a function, there would have to be $p, q \in G$ and $\langle \alpha, n \rangle \in \text{dom } p \cap \text{dom } q$ such that $p(\alpha, n) \neq q(\alpha, n)$. But then there could not exist any function r extending both p and q . But any two elements of G are compatible in P so such r does exist, a contradiction which establishes (i).

(ii) Let $\alpha < \omega_2^M$, $n < \omega$ be arbitrary. Let $D = \{p \in P: \langle \alpha, n \rangle \in \text{dom } p\}$. Then D is dense, since if $p \in P$, either $p \in D$ already or else $p' = p \cup \{\langle \alpha, n, 0 \rangle\}$ is in D and is $\leq p$. By density there is $p \in D \cap G$. Then $\langle \alpha, n \rangle \in \text{dom } p \subseteq \text{dom } g$, proving (ii).

(iii) Let $\alpha < \beta < \omega_2^M$ be arbitrary. Let

$$D = \{p \in P: \exists n \in \omega (\langle \alpha, n \rangle, \langle \beta, n \rangle \in \text{dom } p \wedge p(\alpha, n) \neq p(\beta, n))\}.$$

Then D is dense, since if $p \in P$, then by finiteness of $\text{dom } p$ there is $n \in \omega$ with $\langle \alpha, n \rangle, \langle \beta, n \rangle \notin \text{dom } p$. Setting $p' = p \cup \{\langle \alpha, n, 0 \rangle, \langle \beta, n, 1 \rangle\}$, we have $p' \leq p$ and $p' \in D$. By density there is $p \in D \cap G$. But then $g(\alpha, n) = p(\alpha, n) \neq p(\beta, n) = g(\beta, n)$, proving (iii). (There is no trouble in seeing that the sets D required in (ii) and (iii) can be formed inside M .) $\square$

It is important to notice that 3.2 does not yet tell us that $N \models \neg \text{CH}$. To

get that, we need a function $g \in N$ satisfying (*) and having domain $\omega_2^N \times \omega$. We will in fact show $N \models \neg \text{CH}$ by showing $\omega_2^N = \omega_2^M$. First a simple remark.

If M, N are CTM's with $M \subseteq N$, and $\kappa < \text{OR}^M$ is a cardinal in N , then it must also be a cardinal in M . For if there exist $\lambda < \kappa$ and a function $f \in M$ from λ onto κ , then this same f is present in N , and κ cannot be a cardinal there. If μ is any cardinal in M , we say μ is *preserved* in N if μ is still a cardinal in N , and otherwise μ is *collapsed*. Collapsing occurs when there is a function $f \in N - M$ from a smaller ordinal onto μ .

To prove that $\omega_2^N = \omega_2^M$ in the situation of 3.2, we need to show that ω_1^M and ω_2^M are preserved in N . We do not, by the above remark, have to worry about any *new* cardinals appearing in N . We do have to worry that ω_2^M might be collapsed (and so not be a cardinal at all in N) or that ω_1^M might be collapsed (so that ω_2^M would not be the *second* uncountable cardinal in N). Several preliminaries are required before we can rule out these possibilities.

3.3. DEFINITION. Let P be any PO set, κ any uncountable cardinal. We say P satisfies the κ -*antichain condition*, or is κ -AC, if there is no antichain $A \subseteq P$ of cardinality $\geq \kappa$. Thus trivially P is $(\text{card } P)^+$ -AC. Unfortunately the ω_1 -antichain condition has come to be called the *countable chain condition* (CCC). This usage is confusing, but well established.

3.4. THEOREM. Let M be any CTM, $P \in M$ any PO set, $\kappa \in M$. Suppose $M \models (\kappa \text{ is a regular cardinal} \wedge P \text{ is } \kappa\text{-AC})$. Then $P \Vdash (\kappa^* \text{ is a cardinal})$.

PROOF. Note that $P \Vdash (\kappa^* \text{ is a cardinal})$ is another way of writing $1_P \Vdash (\kappa^* \text{ is a cardinal})$ and is true iff for every M -generic $G \subseteq P$, κ is preserved in $M[G]$. Assume for contradiction that G is generic, and $f \in M[G]$ maps some $\lambda < \kappa$ onto κ . By the Minimality Lemma 2.5, $f = I_G(t)$ for some $t \in \mathcal{P}^M(P \times \lambda \times \kappa)$. By the Truth Lemma 2.9, some $p \in G$ forces (f is a surjection from λ^* to κ^*).

All the following is then true inside M : For $\alpha < \lambda$ let

$$A_\alpha = \{\beta < \kappa : \exists q \leq p (q \Vdash t(\alpha^*) = \beta^*)\}.$$

A_α may be thought of as a set of "possible values of $t(\beta^*)$ ". For $\beta \in A_\alpha$, pick $q(\beta) \leq p$ with $q(\beta) \Vdash t(\alpha^*) = \beta^*$. For distinct β the $q(\beta)$ are incompatible, since they force contradictory things. Since P is κ -AC, it follows $\text{card } A_\alpha < \kappa$. Since κ is regular, $\text{card } A < \kappa$, where $A = \bigcup_{\alpha < \lambda} A_\alpha$. (All this talk of forcing inside M is justified by the Definability Lemma 2.11.)

The above shows $\text{card}^M A < \kappa$. We obtain a contradiction by showing $\kappa \subseteq A$, so that κ cannot be a cardinal in M . To see this, let $\beta < \kappa$ be arbitrary. $\beta = f(\alpha)$ for some $\alpha < \lambda$. By the Truth Lemma, some $q \in G$ forces $t(\alpha^*) = \beta^*$. We may suppose $q \leq p$. (If not, there is $r \in G$ with $r \leq p$ and $r \leq q$. But $r \leq q$ implies that r still forces $t(\alpha^*) = \beta^*$.) Then q is a witness that $\beta \in A_\alpha \subseteq A$. Thus $\kappa \subseteq A$ as asserted. $\square$

Note that in the situation of 3.4, if λ is a cardinal in M with $\kappa \leq \lambda$, then a fortiori $M \models (P \text{ is } \lambda\text{-AC})$, and $P \Vdash (\lambda^* \text{ is a cardinal})$. Thus if $M \models (P \text{ is CCC})$ then all cardinals of M are preserved in all Cohen extensions $M[G]$ for M -generic $G \subseteq P$. Note also that trivially any $P \in M$ is *really* CCC, since it is countable. What matters is whether it is true *inside* M that P is CCC.

3.5. LEMMA. *The α -Cohen PO set is CCC for any ordinal α .*

For the proof we assume the following result:

3.6. COMBINATORIAL LEMMA. *Let κ be a cardinal such that $\kappa^\lambda = \kappa$ for all $\lambda < \kappa$. Let F be a family of $> \kappa$ sets each of cardinality $< \kappa$. Then there exist $E \subseteq F$ of cardinality $> \kappa$ and a fixed set e of cardinality $< \kappa$, such that for all distinct $d, d' \in E$, $d \cap d' = e$.*

The hypothesis on κ is satisfied by $\kappa = \omega$. Assuming CH, it is also satisfied by $\kappa = \omega_1$. The hypothesis implies κ is regular, since $\kappa^{\text{cf } \kappa} > \kappa$ for any cardinal κ . A proof of 3.6 in the case $\kappa = \omega$ can be found in 5.7 of Chapter B.3 or in MARCZEWSKI [1947]. The full 3.6 is an easy generalization.

PROOF OF 3.5 (modulo 3.6). Assume for contradiction there is an uncountable antichain A in the α -Cohen PO set P . For fixed finite $a \subseteq \alpha \times \omega$, there are only finitely many functions from a to $\{0, 1\}$. Thus $F = \{\text{dom } p : p \in A\}$ must be uncountable. Apply 3.6 with $\kappa = \omega$ to obtain an uncountable $E \subseteq F$ and a fixed finite e such that for distinct $d, d' \in E$, $d \cap d' = e$. Since there are only finitely many functions from e to $\{0, 1\}$, there must be $p, q \in A$ with $\text{dom } p, \text{dom } q$ distinct elements of E and p, q agreeing on e . But then $r = p \cup q$ is a function extending both p and q , and so $p, q \in A$ are compatible, a contradiction. $\square$

Now let M, P, G, N be as in 3.2. Applying 3.5 *inside* M , $M \models (P \text{ is CCC})$.

Thus by 3.4 every cardinal of M is preserved in N , and in particular $\omega_2^N = \omega_2^M$, which was the last step required to prove:

3.7. THEOREM (Cohen). *There is a CTM N with $N \models \neg \text{CH}$.*

What does it mean for CH to be true inside a CTM M ? It means that there is a surjection $g \in M$ from ω_1^M onto $\mathcal{P}^M(\omega)$. If such a g does not exist (i.e. $M \models \neg \text{CH}$) we show how to construct an extension N of M in which one does exist.

3.8. DEFINITION. The *anti-Cohen* PO set is the set

$$P = \{p: (p \text{ is a function}) \wedge \text{card dom } p \leq \omega \\ \wedge \text{dom } p \subseteq \omega_1 \wedge \text{range } p \subseteq \mathcal{P}(\omega)\},$$

partially ordered by reverse inclusion.

3.9. LEMMA. *Let M be a CTM, let $P \in M$ be such that $M \models (P \text{ is the anti-Cohen PO set})$, let $G \subseteq P$ be M -generic, $N = M[G]$, $g = \bigcup G \in N$. Then g is a surjection from ω_1^M to $P^M(\omega)$.*

PROOF. Note that what P really is is

$$\{p \in M: (p \text{ is a function}) \wedge \text{card}^M \text{dom } p \leq \omega \\ \wedge \text{dom } p \subseteq \omega_1^M \wedge \text{range } p \subseteq \mathcal{P}^M(\omega)\}.$$

To see that g is a function, argue as in 3.2(i). To see $\text{range } g = P^M(\omega)$ and $\text{dom } g = \omega_1^M$, argue as in 3.2(ii), using the density of $\{p \in P: a \in \text{range } p\}$ for all $a \in \mathcal{P}^M(\omega)$ and the density of $\{p \in P: \alpha \in \text{dom } p\}$ for all $\alpha < \omega_1^M$. $\square$

3.9 does not yet show $N \models \text{CH}$, but to get that it will suffice to show that $\mathcal{P}^N(\omega) = \mathcal{P}^M(\omega)$ and that ω_1^M is preserved in N (so that $\omega_1^N = \omega_1^M$). This requires some preliminaries.

3.10. DEFINITION. Let P be any PO set, κ any uncountable cardinal. P is κ -closed if whenever $\lambda \leq \kappa$ and $p_\xi, \xi < \lambda$, is a decreasing sequence in P (i.e. $p_\eta \leq p_\xi$ when $\xi \leq \eta$), then there is a $p \in P$ which is $\leq$ every p_ξ . P is κ -distributive if any intersection of κ open dense subsets of P is dense. (Trivially such an intersection is open.)

Example. The anti-Cohen PO set P is ω -closed. If we have a countable sequence of functions in P with later members of the sequence extending earlier members, then the union p of all members of the sequence is still a

function with countable domain, hence is an element of P extending every member of the sequence.

3.11. PROPOSITION. *Let P be a PO set, κ an uncountable cardinal. Then:*

- (i) *If P is κ -closed, then P is κ -distributive.*
- (ii) *If κ is singular, and P is λ -closed (or λ -distributive) for every $\lambda < \kappa$, then P is κ -closed (resp. κ -distributive).*

PROOF. (i) Suppose P is κ -closed and $D_\xi, \xi < \kappa$, are open dense subsets of P . To show their intersection dense, consider an arbitrary $p \in P$. We form a decreasing sequence $p_\xi, \xi \leq \kappa$, of elements of P as follows: Let $p_0 = p$. If p_ξ is defined, pick $p_{\xi+1} \leq p_\xi$ and belonging to D_ξ (such exists by density). If $\lambda \leq \kappa$ and $\text{Lim}(\lambda)$ and p_ξ is defined for $\xi < \lambda$, let p_λ be $\leq$ all $p_\xi, \xi < \lambda$ (such exists by κ -closure). Then we have found $p_\kappa \leq p$ with $p_\kappa \in \bigcap_{\xi < \kappa} D_\xi$ (by openness, since $p_\kappa \leq p_{\xi+1} \in D_\xi$). This proves the required density.

(ii) For closure, note that from any decreasing sequence $p_\xi, \xi < \kappa$, we can extract a sequence $q_\eta, \eta < \text{cf } \kappa$, such that for every p_ξ there is a q_η with $q_\eta \leq p_\xi$. For density, note that any intersection of κ sets can be rewritten as an intersection of $\text{cf } \kappa$ sets, each of which is an intersection of $< \kappa$ sets. $\square$

3.12. THEOREM. *Let M be a CTM, $P \in M$ a PO set, κ a cardinal in M . Suppose $M \models (P \text{ is } \kappa\text{-distributive})$. Let $G \subseteq P$ be M -generic, $N = M[G]$, and $f \in N$ a function with $\text{dom } f = \kappa$, $\text{range } f \subseteq M$. Then $f \in M$.*

PROOF. By the Minimality Lemma, $f = I_G(t)$ for some $t \in M$, say $t \in \mathcal{P}^M(P \times \kappa \times b)$. Assume for contradiction $f \notin X = \{h \in P^M(\kappa \times b) : h \text{ is a function}\}$. By the Truth Lemma, some $p \in G$ forces $(t \text{ is a function} \wedge t \notin X^*)$. We obtain a contradiction by finding $q \leq p$ and $h \in X$ such that q forces $\forall \alpha < \kappa^*(t(\alpha) = h^*(\alpha))$, i.e. $t = h^*$.

All the following is true inside M : For $\alpha < \kappa$, let $D_\alpha = \{q \leq p : \exists c \in b (q \Vdash t(\alpha^*) = c^*)\}$. Then D_α is open dense below p in P . Openness is clear. To prove density, consider an arbitrary $q \leq p$. Since $q \Vdash \exists c \in b (t(\alpha^*) = c)$, there are $c \in b$ and $r \leq q$ such that $r \Vdash t(\alpha^*) = c^*$ (this by 2.10(v)), whence $r \in D_\alpha$. By κ -distributivity, $\bigcap_{\alpha < \kappa} D_\alpha$ is dense below p . (More precisely, apply distributivity to the sets $E_\alpha = \{q \in P : p, q \text{ are incompatible} \vee q \in D_\alpha\}$, which are fully dense in P ; cf. Lemma 2.13.) Now if q belongs to all the D_α and we define

$$h = \{(\alpha, c) \in \kappa \times b : q \Vdash t(\alpha^*) = c^*\},$$

then $h \in X$ and clearly $q \Vdash \forall \alpha < \kappa^*(t(\alpha) = h^*(\alpha))$ as required. (This

whole argument “took place inside M ”. All the talk about forcing inside M involves tacit use of the Definability Lemma.) $\square$

3.13. COROLLARY. *Let the notation be as in 3.12. Then:*

(i) $P^N(\kappa) = P^M(\kappa)$.

(ii) *Every cardinal in $M \leq (\kappa^+)^M$ is preserved in N .*

PROOF. (i) If there were $a \in P^N(\kappa) - P^M(\kappa)$, its characteristic function would be a counterexample to 3.12.

(ii) If λ, μ were cardinals in M with $\mu < \lambda \leq (\kappa^+)^M$ and $f \in N$ were a surjection from μ to λ , then the trivial extension g of f to a function with $\text{dom } g = \kappa$, obtained by setting $g(\alpha) = 0$ for $\mu \leq \alpha < \kappa$, would be a counterexample to 3.12. $\square$

Now let M, P, G, N be as in 3.9. Then $M \models (P \text{ is } \omega\text{-closed})$. By 3.13, $P^N(\omega) = P^M(\omega)$ and ω_1^M is preserved in N , which were the facts needed to prove:

3.14. THEOREM (Gödel). *There is a CTM N with $N \models \text{CH}$.*

Gödel's original proof of Theorem 3.14 antedated the method of forcing by a quarter century. His proof gives a model in which we have not only CH, but also GCH and an even stronger principle, the so-called Axiom of Constructibility ($V = L$). See Chapter B.5 for an account of this work.

The following technical result will be used often below:

3.15. THEOREM. *Let M be a CTM, $P \in M$ a PO set, and $\kappa, \lambda, \mu, \nu$ cardinals in M . Suppose $M \models (\nu = \kappa^{\lambda\mu} \wedge \text{card } P = \kappa \wedge P \text{ is } \lambda^+\text{-AC})$. Then $p \Vdash 2^\mu \leq \nu$.*

PROOF. Let $G \subseteq P$ be M -generic, $N = M[G]$. We show $(2^\mu)^N \leq \nu$ by showing that inside N every subset of μ can be obtained using I_G from elements of a certain set $S \in M$ with $\text{card}^M S \leq \nu$. Indeed, let

$$S = \{f \in M : (f \text{ is a function}) \wedge \text{dom } f \subseteq P \times \mu \wedge \text{range } f \subseteq \{0, 1\} \wedge$$

$$\forall \alpha < \mu (A(\alpha, f) = \{p \in P : \langle p, \alpha \rangle \in \text{dom } f \text{ is a maximal antichain})\}.$$

We can see $S \in M$ by appealing to the Definability Lemma.

All the following is true inside M : Any antichain in P has cardinality $\leq \lambda$. Since $\text{card } P = \kappa$, the number of antichains $A \subseteq P$ is $\leq \kappa^\lambda$. Every $f \in S$ is completely determined by the sequence of μ antichains $A(\alpha, f)$, $\alpha < \mu$. Thus $\text{card } S \leq (\kappa^\lambda)^\mu = \kappa^{\lambda\mu} = \nu$.

All this was true inside M , showing $\text{card}^M S \leq \nu$, hence $\text{card}^N S \leq \nu$. Further, all the following is true inside N : For each $\alpha < \mu$ and $f \in S$, $A(\alpha, f) \cap G$ has just one element (by 2.15(i)), call it $q(\alpha, f)$. Define $J(f) = \{\alpha < \mu : f(q(\alpha, f), \alpha) = 0\}$. Then J maps S into $\mathcal{P}(\mu)$.

We complete the proof by showing the $J \in N$ just defined maps S onto $\mathcal{P}^N(\mu)$. To see this, let $a \in \mathcal{P}^N(\mu)$ be arbitrary. $a = I_G(t)$ for some $t \in \mathcal{P}^M(P \times \mu)$.

All the following is then true inside M : By Zorn's Lemma, there is an $f \subseteq P \times \mu \times \{0, 1\}$ maximal with respect to the property:

(if $\langle p, \alpha, 0 \rangle \in f$, then $p \Vdash \alpha^* \in t$) $\wedge$ (if $\langle p, \alpha, 1 \rangle \in f$, then $p \Vdash \alpha^* \notin t$) $\wedge$

$A(\alpha, f) = \{p : \langle p, \alpha \rangle \in \text{dom } f\}$ is an antichain for all α .

Note that the first two conditions imply f is a function. We claim the $A(\alpha, f)$ are actually *maximal* antichains. For if for some α , some $q \in P$ were incompatible with all $p \in A(\alpha, f)$, then since $q \Vdash (\alpha^* \in t \vee \alpha^* \notin t)$, there would be an $r \leq q$ such that either $r \Vdash \alpha^* \in t$ or $r \Vdash \alpha^* \notin t$. In the former case, $f \cup \{\langle r, \alpha, 0 \rangle\}$ would be a counterexample to the maximality of f . In the latter case, $f \cup \{\langle r, \alpha, 1 \rangle\}$ would be. This contradiction shows the $A(\alpha, f)$ are maximal antichains as claimed, and hence $f \in S$.

It remains to show $J(f) = a$. Let $\alpha < \mu$ be arbitrary. Suppose first $\alpha \in a$. By the Truth Lemma, some $p \in G$ forces $\alpha^* \in t$. Now we cannot have $f(q(\alpha, f), \alpha) = 1$, for then by the defining property of f , $q(\alpha, f) \in G$ would force $\alpha^* \notin t$, making $q(\alpha, f)$ incompatible with $p \in G$, a contradiction. So we must have $f(q(\alpha, f), \alpha) = 0$, and $\alpha \in J(f)$. Similarly, if $\alpha \in \mu - a$, then $\alpha \notin J(f)$. Thus $J(f) = a$ as required to complete the proof. $\square$

3.16. Consequences of 3.15

Let M be a CTM with $M \models \text{GCH}$. The work of Gödel mentioned after Theorem 3.14 provides such an M .

(i) Let $P \in M$ be the ω_2^M -Cohen conditions, $G \subseteq P$ M -generic, $N = M[G]$. We have seen $N \models 2^\omega > \omega_1$. Now applying 3.15 with $\kappa = \nu = \omega_2^M$ and $\lambda = \mu = \omega$, we see $N \models 2^\omega = \omega_2$ exactly. Next applying 3.15 with $\kappa = \nu = \omega_2^M$, $\lambda = \omega$, and $\mu = \omega_1^M$, we see $N \models 2^{\omega_1} = \omega_2$. (Note GCH implies $\omega_2^{\omega_1} = \omega_2^{\omega} = \omega_2$.) This establishes the consistency of $2^\omega = 2^{\omega_1}$.

(ii) Similar use of the ω_3^M -Cohen conditions gives a model with $2^\omega = \omega_3$. In fact we can get any "reasonable" value for 2^ω . (It has long been known that $2^\omega \neq \omega_\omega$. Use of the $(\omega_\omega)^M$ -Cohen conditions turns out to make $2^\omega = \omega_{\omega+1}$.)

(iii) Let

$$P = \{p \in M: (p \text{ is a function}) \wedge \text{card}^M \text{ dom } p \leq \omega \wedge \\ \text{dom } p \subseteq \omega_3^M \times \omega_1^M \wedge \text{range } p \subset \{0, 1\}\}.$$

It is easy to see $M \models (P \text{ is } \omega\text{-closed})$. Using GCH inside M and 3.6, it can be seen that $M \models (P \text{ is } \omega_2^M\text{-AC})$. Thus if $G \subseteq P$ is M -generic, then by 3.4 and 3.13, every cardinal of M is preserved in $N = M[G]$. It is then not hard to see $N \models 2^{\omega_1} > \omega_2$, and using 3.15 it can even be established that $N \models 2^{\omega_1} = \omega_3$ exactly. By ω -closure and 3.13, $\mathcal{P}^N(\omega) = \mathcal{P}^M(\omega)$, so $N \models 2^\omega = \omega_1$. To get combinations like $2^{\omega_1} = \omega_3$ and $2^\omega = \omega_2$ will require the more sophisticated methods of Section 5 below.

4. Useful combinatorial principles

The principles to be discussed in this section have proved useful everywhere from universal algebra to general topology. (E.g. see Chapter B.7.) We show each principle (relatively) consistent by constructing a model for it. In most cases consistency can also be established by deriving the principle from $V = L$ (see Chapter B.5), but these derivations are usually longer than the forcing constructions used here.

4.1. DEFINITION. Let κ be a regular uncountable cardinal. A κ *Kurepa tree* is a tree T of height κ whose levels all have cardinality $< \kappa$, and which has $> \kappa$ branches. The κ *Kurepa Hypothesis*, $\text{KH}(\kappa)$, is the proposition that κ Kurepa trees exist. We aim to show $\text{KH}(\omega_1)$ is consistent.

Let P be the set of all pairs $\langle T_p, l_p \rangle$ where:

- (1) T_p is a tree.
- (2) The elements of $|T_p|$ are ordinals $< \kappa$.
- (3) Every level of T_p has cardinality $< \kappa$.
- (4) T_p has height a successor ordinal $\alpha_p + 1 < \kappa$, i.e. T_p has a top level, the α_p -th.

- (5) l_p is a bijection from a subset of κ^+ to the top level of T_p .

Partially order P by setting $p < q$ iff:

- (6) T_p is an end extension of T_q , i.e. the levels of T_p up to the α_q -th are identical with the levels of T_q , but T_p (possibly) has new levels above the α_q -th.

- (7) $\text{dom } l_p \supseteq \text{dom } l_q$.

- (8) For every $\rho \in \text{dom } l_q$, $l_q(\rho) \leq l_p(\rho)$ in T_p .

Thus ordered P is called the $\text{KH}(\kappa)$ PO set.

If $p \in P$, T_p may be thought of as part of a Kurepa tree T we would like

to construct, and l_p as a labeling indicating for certain $\rho < \kappa^+$ which element of the top level of T_p belongs to the ρ -th branch through T (in some list of κ^+ branches we are trying to construct).

4.2. LEMMA. *Let κ be regular and uncountable, P the $\text{KH}(\kappa)$ PO set. Then P is λ -closed for all $\lambda < \kappa$.*

PROOF. Let $\lambda < \kappa$ and let $p_\xi, \xi < \lambda$, be a decreasing sequence in P . Write T_ξ for the tree part of p_ξ , and l_ξ, α_ξ similarly to avoid double subscripts. Note that the sequence of α_ξ is nondecreasing. Since T_η is an end extension of T_ξ for $\xi \leq \eta$, the T_ξ fit together to form a single tree T of height $\alpha = \sup\{\alpha_\xi: \xi < \lambda\}$. Let $d = \bigcup_{\xi < \lambda} \text{dom } l_\xi$. For $\rho \in d$, let

$$b(\rho) = \{a \in T: \exists \xi < \lambda (\rho \in \text{dom } l_\xi \wedge a \leq l_\xi(\rho))\}.$$

Since $l_\xi(\rho) \leq l_\eta(\rho)$ for $\xi \leq \eta < \lambda$ and $\rho \in \text{dom } l_\xi$, $b(\rho)$ is a branch through T . Moreover since the maps l_ξ are injections, $b(\rho) \neq b(\sigma)$ for $\rho \neq \sigma$. Form a tree T' by adding to T a new level at the very top containing for each $\rho \in d$ an element a_ρ which is $\geq$ every $a \in b(\rho)$. Define a map l with domain d by setting $l(\rho) = a_\rho$. It is easily seen that $p_\lambda = \langle T', l \rangle$ is an element of $P \leq$ every p_ξ . $\square$

4.3. PROPOSITION. *Let κ be an uncountable cardinal such that $\kappa^\lambda = \kappa$ for all $\lambda < \kappa$, and P the $\text{KH}(\kappa)$ PO set. Then P is κ^+ -AC.*

PROOF. Suppose $A \subseteq P$ has cardinality κ^+ . We show A is not an antichain. The assumption on κ implies that there are only κ subsets of κ of cardinality $< \kappa$. Moreover for a fixed subset of cardinality λ , there are only $2^\lambda \leq \kappa^\lambda = \kappa$ ways to partially order it and make it into a tree. Thus there are only κ trees satisfying the conditions on T_p in the definition of the $\text{KH}(\kappa)$ PO set. So there exist $A' \subseteq A$ of cardinality κ^+ and a fixed tree T such that $T_p = T$ for all $p \in A'$.

For fixed $d \subseteq \kappa^+$ of cardinality $\lambda < \kappa$ there are no more than κ bijections from d to the top level of T , hence no more than κ $p \in A'$ with $\text{dom } l_p = d$. Thus $D = \{\text{dom } l_p: p \in A'\}$ has cardinality κ^+ , and we can apply Lemma 3.6 to get an $E \subseteq D$ with $\text{card } E = \kappa^+$ and a fixed e such that $d \cap d' = e$ for all distinct $d, d' \in E$. Since there are only κ maps from this e to the top level of T , there must be $p, q \in A'$ with $\text{dom } p, \text{dom } q$ distinct elements of E , and p, q agreeing on e . We complete the proof by showing such p, q are compatible.

Let us add a new level to the top of T containing one new point above

each element $l_p(\rho)$ for $\rho \in e$, and two new points above each element $l_p(\rho)$ for $\rho \in \text{dom } l_p - e$. (Note any such element is also of the form $l_q(\sigma)$ for some $\sigma \in \text{dom } l_q - e$.) This forms a new tree T' . Define a map l' with domain $\text{dom } l_p \cup \text{dom } l_q$ by setting:

$$l'(\rho) = \begin{cases} \text{the unique point above } l_p(\rho), & \text{if } \rho \in e, \\ \text{the 1st point above } l_p(\rho), & \text{if } \rho \in \text{dom } l_p - e, \\ \text{the 2nd point above } l_q(\rho), & \text{if } \rho \in \text{dom } l_q - e. \end{cases}$$

It is easily seen that $\langle T', l' \rangle$ is $\leq$ both p and q in P as required. $\square$

We leave it to the reader to check that if κ is regular, P the $\text{KH}(\kappa)$ PO set, then the sets $D_\alpha = \{p \in P : \alpha_p > \alpha\}$, for $\alpha < \kappa$, and the sets $E_\rho = \{p \in P : \rho \in \text{dom } l_p\}$, for $\rho < \kappa^+$, are dense.

4.4. THEOREM (Stewart). *There is a CTM N with $N \models \text{KH}(\omega_1)$.*

PROOF. The reader may prove, or trust us, that the notions of being a tree, and of level, height, and branch for trees are absolute. (Any proof would invoke 1.6(iii) and (iv).) Thus we do not need to distinguish between application of the notions inside and outside a CTM.

Let M be a CTM with $M \models \text{GCH}$. Let $\kappa = \omega_1^M$. Let $P \in M$ be such that $M \models P$ is the $\text{KH}(\kappa)$ PO set. Let $G \subseteq P$ be M -generic, $N = M[G]$, and $T = \bigcup_{p \in G} T_p \in N$. We show $N \models T$ is a κ Kurepa tree. Note that by 4.2 and 4.3 and lemmas of Section 3, all cardinals of M are preserved in N , and so $\kappa = \omega_1^N$, $\omega_2^M = \omega_2^N$.

If $p, q \in P$ are compatible, then either T_p is an end extension of T_q or vice versa. Since elements of G are compatible, it follows that T is a tree, and an end extension of all the $T_p, p \in G$. Moreover, any level of T is a level of T_p for some $p \in G$, hence has cardinality $< \kappa$ inside N . For $\alpha < \kappa$, the set D_α defined above (after the proof of 4.3) is dense, so $D_\alpha \cap G \neq \emptyset$. This implies $\text{height}(T) > \alpha$. Thus $\text{height}(T) = \kappa$.

If $p, q \in G$ and $\rho \in \text{dom } l_p \cap \text{dom } l_q$, then by compatibility of p, q , $l_p(\rho)$ and $l_q(\rho)$ are comparable in T . (They are both $\leq l_r(\rho)$ for any $r \leq$ both p, q .) If ρ, σ are distinct elements of $\text{dom } l_p$, then $l_p(\rho)$ and $l_p(\sigma)$ are incompatible in T . (They are distinct elements of the same level of T , the α_p -th.) If $\alpha < \kappa$, $\rho < \omega_2^M$, and E_ρ is as defined above (after 4.3), then by density there is $p \in D_\alpha \cap E_\rho \cap G$, and so $l_p(\rho)$ is defined and of level $> \alpha$ in T . These observations show that, setting

$$B(\rho) = \{a \in T : \exists p \in G (\rho \in \text{dom } p \wedge a \leq l_p(\rho))\} \quad \text{for } \rho < \omega_2^M,$$

$B(\rho)$ is a branch through T , and $B(\rho) \neq B(\sigma)$ for distinct ρ, σ . Thus $\{B(\rho): \rho < \omega_2^M\}$ provides, inside N , a family of $> \kappa$ branches through T , as required to show $N \models \text{KH}(\kappa)$. $\square$

Simple variants of the above construction give $\text{KH}(\omega_2)$, $\text{KH}(\omega_3)$, etc. We can also get an ω_1 Kurepa tree with ω_3 or more branches, though this involves making $2^{\omega_1} > \omega_2$, since no tree of cardinality κ can have more than 2^κ branches. A subtler variant is the following:

4.5. THEOREM (Silver). *There is a CTM N with $N \models (2^{\omega_1} > \omega_2 \wedge \text{there exists an } \omega_1 \text{ Kurepa tree with exactly } \omega_2 \text{ branches})$.*

PROOF. Let M, P, G, N, T be as in the proof of Theorem 4.4. Thus inside N , T is an ω_1 Kurepa tree. We have $N \models 2^\omega = \omega_1$, since this holds in M and (by closure conditions on P) $\mathcal{P}^N(\omega) = \mathcal{P}^M(\omega)$. We also have $N \models 2^{\omega_1} = \omega_2$, using GCH inside M and 3.17 (with $\kappa = \nu = \omega_2^M = \omega_2^N$, $\lambda = \mu = \omega_1^M = \omega_1^N$). Thus $N \models T$ has exactly ω_2 branches.

Now let $Q \in N$ be $\{p: p \text{ is a function } \wedge \text{card}^N \text{ dom } p \leq \omega \wedge \text{dom } P \subseteq \omega_3^N \times \omega_1^N \wedge \text{range } p \subseteq \{0, 1\}\}$, partially ordered by reverse inclusion. We remarked at the end of Section 3 (see 3.16(iii)) that $N \models (Q \text{ is } \omega\text{-closed} \wedge Q \text{ is } \omega_2\text{-AC})$. We also saw that if $H \subseteq Q$ is N -generic, then all cardinals of N are preserved in $N[H]$, and $N[H] \models 2^{\omega_1} = \omega_3$. Since all cardinals are preserved, T is still an ω_1 Kurepa tree inside $N[H]$. To show $N[H] \models T$ has exactly ω_2 branches, it suffices to show that any branch through T in $N[H]$ already belongs to N . This, in slightly different notation, is the content of the following:

4.6. LEMMA. *Let M be any CTM, $P \in M$ a PO set, $\kappa \in M$, $T \in M$. Suppose $M \models (\kappa \text{ is a successor cardinal } \wedge P \text{ is } \lambda\text{-closed for all } \lambda < \kappa \wedge T \text{ is a tree } \wedge \text{height}(T) = \kappa \wedge \text{every level of } T \text{ has cardinality } < \kappa)$. Let $G \subseteq P$ be M -generic, $N = M[G]$. Then every branch through T in N already belongs to M .*

PROOF. For simplicity consider the case $\kappa = \omega_1^M$. Let $X = \{B \in M: B \text{ is a branch through } T\}$. Assume for contradiction $B \in N$ is a branch through T and $B \notin X$. Then $B = I_G(t)$ for some $t \in \mathcal{P}^M(P \times T)$. Call p good if $p \Vdash (t \text{ is a branch through } T^* \wedge t \notin X^*)$. Note that there is a good $p \in G$. Note also:

- (i) If p is good and $q \leq p$, then q is good.
- (ii) If p is good, $p \Vdash a^* \in t$, and $b \leq a$ in T , then $p \Vdash b^* \in t$.

(iii) If p is good, and $p \Vdash a^* \in t$, $p \Vdash b^* \in t$, then a, b are comparable in T .

(iv) If p is good, and $\alpha < \kappa$, then there exist $q \leq p$ and $a \in T_\alpha$ such that $q \Vdash a^* \in t$. (Since $p \Vdash \exists x \in T_\alpha^* (x \in t)$.)

(v) If p is good, and $\alpha < \kappa$, then there exist β , $\alpha < \beta < \kappa$, and $q, r \leq p$, and distinct $a, b \in T_\beta$, such that $q \Vdash a^* \in t$ and $r \Vdash b^* \in t$.

To see (v), suppose no such β, q, r, a, b can be found. By (i)–(iv) it follows $C = \{a \in T : \exists q \leq p (q \Vdash a^* \in t)\}$ is a branch through T . Moreover $C \in M$. (This implicitly uses the Definability Lemma.) But it is easily seen that $p \Vdash t = C^* \in X^*$, contrary to the goodness of p .

Now all the following is true inside M : We may form for every finite sequence s of 0's and 1's a good $p(s) \in P$, and $\alpha(s) < \kappa$, and an $a(s) \in T_{\alpha(s)}$ such that $p(s) \Vdash (a(s))^* \in t$, as follows: For the empty sequence $\emptyset$, let $p(\emptyset) =$ any good p , $\alpha(\emptyset) = 0$, $a(\emptyset) =$ the unique element of T_0 , i.e. the minimum element in T . If $p(s)$, $\alpha(s)$, $a(s)$ are defined, then by (v) above we can find β , $\alpha(s) < \beta < \kappa$, and $p(s0)$, $p(s1) \leq p$, and distinct $a(s0)$, $a(s1) \in T_\beta$ with $p(si) \Vdash a(si)^* \in t$ for $i = 0, 1$. Set $\alpha(s0) = \alpha(s1) = \beta$. By (iii) above, $a(s) \leq a(s0), a(s1)$ in T . Now for every infinite sequence S of 0's and 1's we can by countable closure find $p(S) \in P$ with $p(S) \leq p(S \upharpoonright n)$ for all $n < \omega$. Let $\alpha = \sup\{\alpha(s) : s \text{ a finite sequence of 0's and 1's}\}$. By (iv) above, for every S there exist $q(S) \leq p(S)$ and $a(S) \in T_\alpha$ such that $q(S) \Vdash a(S)^* \in t$. By construction $a(s0), a(s1)$ were chosen incompatible in T . By (iii), $a(S \upharpoonright n) \leq a(S)$ for all $n < \omega$. Hence for $S \neq S'$, $a(S) \neq a(S')$. But then $\text{card } T_\alpha \geq 2^\omega \geq \omega_1$.

All this was true inside M , showing $\text{card}^M T_\alpha > \omega_1^M$, contrary to hypothesis. This contradiction establishes 4.6 and 4.5. $\square$

The above proof comes from SILVER [1971]. For a different forcing argument, see JECH [1971]. We now turn to another variant of KH.

4.7. DEFINITION. If T is a tree, $\alpha < \text{height}(T)$, and b an element of T of level $> \alpha$ (or a branch through T), we mean by $\pi_\alpha(b)$ the unique $a \in T_\alpha$ with $a \leq b$ (resp., with $a \in b$).

Let κ be a regular uncountable cardinal. $W(\kappa)$ is the proposition that there exist:

- (1) A κ Kurepa tree T ,
- (2) a family F of $> \kappa$ branches through T ,
- (3) a function W with domain κ ,

such that for all $\alpha < \kappa$, $W(\alpha)$ is a family of $< \kappa$ subsets of T_α , and for any

$S \subseteq F$ with $\text{card } S < \kappa$, there exists $\alpha < \kappa$, such that for any β with $\alpha < \beta < \kappa$, $\{\pi_\beta(B): B \in S\} \in W(\beta)$.

Let P be the set of quadruples $p = \langle T_p, l_p, W_p, S_p \rangle$ such that:

- (4) $\langle T_p, l_p \rangle$ belongs to the $\text{KH}(\kappa)$ PO set,
- (5) W_p is a function with domain height $(T_p) = \alpha_p + 1$,
- (6) $W_p(\alpha)$ is a family of $< \kappa$ subsets of the α -th level of T_p for $\alpha \in \text{dom } W_p$,
- (7) S_p is a family of $< \kappa$ subsets of $\text{dom } l_p$.

Partially order P by setting $p \leq q$ iff:

- (8) $\langle T_p, l_p \rangle < \langle T_q, l_q \rangle$ in the $\text{KH}(\kappa)$ PO set,
- (9) W_p extends W_q ,
- (10) $S_p \supseteq S_q$,
- (11) for every α with $\alpha_q < \alpha \leq \alpha_p$ and every $S \in S_q$,

$$\{\pi_\alpha(l_p(\rho)): \rho \in S\} \in W_p(\alpha).$$

Thus ordered P is called the $W(\kappa)$ PO set. The proof of the following (which closely resembles that of 4.2 and 4.3) is left to the reader:

4.8. LEMMA. *Let κ be a regular uncountable cardinal, P the $W(\kappa)$ PO set. Then:*

- (i) P is λ -closed for all $\lambda < \kappa$.
- (ii) If $\kappa^\lambda = \kappa$ for all $\lambda < \kappa$, then P is κ^+ -AC.
- (iii) For $\alpha < \kappa$, $D_\alpha = \{p: \alpha_p > \alpha\}$ is dense. For $S \subseteq \kappa^+$ with $\text{card } S < \kappa$, $E_S = \{p: S \subseteq \text{dom } l_p \wedge S \in S_p\}$ is dense.

4.9. THEOREM (Silver). *There is a CTM N with $N \models W(\omega_1)$.*

PROOF. Let M be a CTM with $M \models \text{GCH}$. Let $\kappa = \omega_1^M$. Let $P \in M$ be such that $M \models P$ is the $W(\kappa)$ PO set. Let $G \subseteq P$ be M -generic, $N = M[G]$. Note that all cardinals of M are preserved in N .

Let $T \in N$ be $\bigcup_{p \in G} T_p$. For $\rho < \omega_2^M = \omega_2^N$ let $B(\rho)$ be the branch through T defined in the proof of Theorem 4.4. Let $F = \{B(\rho): \rho < \omega_2^M\}$. For $\alpha < \omega_1^M = \omega_1^N$, let $W(\alpha) = W_p(\alpha)$ for some $p \in D_\alpha \cap G$, where D_α is as in 4.8(iii). This definition of $W(\alpha)$ is independent of choice of p by compatibility of elements of G and the fact that if p, q are compatible, then W_p extends W_q or vice versa. We claim T, F, W are as required to make $W(\omega_1)$ true inside N .

To see this, let $S \subseteq \mathcal{P}^N(F)$ have $\text{card}^N S = \omega$. Let $S' = \{\rho: B(\rho) \in S\}$. By the closure condition on P and Lemma 3.12, any $f \in N$ mapping ω onto S' belongs to M . Hence $S' \in M$. By density of the set E_S , defined in 4.8(iii),

there is $p \in G$ with $S' \in S_p$. It suffices to show that if $\alpha_p < \alpha$, then $\{\pi_\alpha(B): B \in S\} \in W(\alpha)$. To see this, consider $q \in D_\alpha \cap G$ with $q \geq p$. The last clause in the definition of the order on P guarantees that $\{\pi_\alpha(B): B \in S\} = \{\pi_\alpha(l_q(\rho)): \rho \in S'\} \in W_q(\alpha) = W(\alpha)$. $\square$

4.10. DEFINITION. Let κ be an uncountable cardinal. $\square(\kappa)$ is the proposition that there exists a function C with domain $\{\alpha < \kappa^+: \text{Lim}(\alpha)\}$ such that for all $\alpha \in \text{dom } C$:

- (i) $C(\alpha) \subseteq \alpha$ and is CUB in α .
- (ii) If $\text{cf } \alpha < \kappa$, then $\text{card } C(\alpha) < \kappa$.
- (iii) If β is a limit point in $C(\alpha)$, i.e. if $\beta < \alpha$ and $C(\alpha) \cap \beta$ is cofinal in β , then $C(\beta) = C(\alpha) \cap \beta$.

In case κ is singular, the antecedent of (ii) is always fulfilled, and so (ii) reduces to:

- (ii') $\text{card } C(\alpha) < \kappa$.

We aim to prove that $\square(\omega_1)$, $\square(\omega_\omega)$, etc. are consistent.

Let P be the set of all functions p with domain $\{\alpha \leq \alpha(p): \text{Lim}(\alpha)\}$ for some limit ordinal $\alpha(p) < \kappa^+$, and satisfying (i)–(iii) above for all $\alpha \in \text{dom } p$. Partially order P by reverse inclusion. Thus ordered P is called the $\square(\kappa)$ PO set.

4.11. LEMMA. *Let κ be an uncountable cardinal, P the $\square(\kappa)$ PO set. Then P is κ -distributive.*

PROOF. P is not κ -closed, but we can prove distributivity directly. First consider $\lambda < \kappa$ and open dense $D_\xi \subseteq P$, $\xi < \lambda$. We show $\bigcap_{\xi < \lambda} D_\xi$ is dense. This proves λ -distributivity for all $\lambda < \kappa$. In case κ is regular, the same proof works for $\lambda = \kappa$. In case κ is singular, we get κ -distributivity by 3.11(ii).

Let $p \in P$ be arbitrary. We attempt to construct a decreasing sequence p_ξ , $\xi \leq \lambda$, in P as follows: Let $p_0 = p$. At a successor ordinal $\xi + 1$, if p_ξ is defined, choose $p_{\xi+1} < p_\xi$ and belonging to D_ξ . At a limit ordinal ζ , if p_ξ has been defined for all $\xi < \zeta$, then $f = \bigcup_{\xi < \zeta} p_\xi$ is a function satisfying 4.10(i)–(iii) and having as domain the set of all limit ordinals $< \alpha$, where $\alpha = \sup\{\alpha(p_\xi): \xi < \zeta\}$. Let g be the function extending f with domain $\{\beta < \alpha: \text{Lim}(\beta)\}$ obtained by setting $g(\alpha) = \{\alpha(p_\xi): \xi < \zeta\}$. If this g still satisfies 4.10(i)–(iii), set $p_\zeta = g$. Otherwise p_ζ is undefined and our inductive construction breaks down.

If this process never breaks down, then p_λ is defined and belongs to all the D_ξ . Since our original p was arbitrary, this proves the required density of $\bigcap_{\xi < \lambda} D_\xi$.

So assume for contradiction the process does break down at some limit ordinal $\zeta < \lambda$. This can only happen if, in the notation above, setting $g(\alpha) = \{\alpha(p_\xi) : \xi < \zeta\}$ results in a violation of 4.10(i)–(iii).

But obviously $g(\alpha)$ is cofinal in α . Now if $\xi < \eta < \zeta$, then $\alpha(p_\xi) < \alpha(p_\eta)$ since $p_\xi < p_\eta$. So if $\beta < \alpha$ is a limit point of $g(\alpha)$, β has the form $\sup\{\alpha(p_\xi) : \xi < \eta\}$ for some limit $\eta < \zeta$. But then by construction $\alpha(p_\eta) = \beta$, and $\beta \in g(\alpha)$. Thus $g(\alpha)$ is closed in α , and 4.10(i) is not violated.

Moreover, by construction for limit $\eta < \zeta$, $g(\alpha(p_\eta)) = p_\eta(\alpha(p_\eta)) = \{\alpha(p_\xi) : \xi < \eta\} = g(\alpha) \cap \alpha(p_\eta)$. Thus 4.10(iii) is not violated either. Nor is 4.10(ii), since $\text{card } g(\alpha) \leq \text{card } \alpha \leq \lambda < \kappa$. We have reached a contradiction, which shows that our inductive construction never breaks down. $\square$

4.12. LEMMA. *Let κ , P be as in Lemma 4.11. Then for any limit ordinal $\alpha < \kappa^+$, $D_\alpha = \{p : \alpha(p) \geq \alpha\}$ is open dense in P .*

PROOF. Openness is clear. We prove density by induction on α . If there is a greatest limit ordinal $\beta < \alpha$ and D_β is dense, we have $\alpha = \beta + \omega$. Moreover any element p of D_β can be trivially extended to an element q of D_α by setting $q(\alpha) = \{\beta + n : n < \omega\}$, so D_α is dense. If α is a limit of limit ordinals and D_β is open dense for all limits $\beta < \alpha$, then $D_\alpha = \bigcap_{\beta < \alpha} D_\beta$ is dense by κ -distributivity. $\square$

Notice that if we assume GCH, the cardinality of the $\square(\kappa)$ PO set is κ^+ , so it is trivially κ^{++} -AC.

4.13. THEOREM (Jensen). *There exists a CTM N with $N \models \square(\omega_1)$, and the same is true for $\square(\omega_2)$, $\square(\omega_\omega)$, etc.*

PROOF. Let M be a CTM with $M \models \text{GCH}$. Let $\kappa = \omega_1^M$ or ω_ω^M or what have you. Let $P \in M$ be such that $M \models P$ is the $\square(\kappa)$ PO set. Let $G \subseteq P$ be M -generic, $N = M[G]$, $C = \bigcup G \in N$. By the distributivity and chain conditions on P , all cardinals of M are preserved in N . It is easily verified that C is a function (cf. Lemma 3.2(i)), with $\text{dom } C = (\kappa^+)^M$. By preservation of cardinals, $(\kappa^+)^N = (\kappa^+)^M$. It is then easily verified that C satisfies 4.10(i)–(iii), recalling that sets have the same cardinalities in M and N , and that being CUB is an absolute property. Details are left to the reader. $\square$

4.14. DEFINITION. Let κ be a regular uncountable cardinal. $E(\kappa)$ is the proposition that there exists a stationary set $E \subseteq \kappa$ such that $E \cap \alpha$ is not stationary in α for any limit ordinal $\alpha < \kappa$.

Let P be the set of pairs $p = \langle E_p, \alpha_p \rangle$ such that $\alpha_p < \kappa$, $E_p \subseteq \alpha_p$, and

$E_p \cap \alpha$ is not stationary in α for any limit ordinal $\alpha \leq \alpha_p$. Partially order P by setting $p \leq q$ iff $\alpha_p \geq \alpha_q$ and $E_p \cap \alpha_q = E_q$. Thus ordered P is called the $E(\kappa)$ PO set.

4.15. LEMMA. *Let κ be a regular uncountable cardinal, P the $E(\kappa)$ PO set. Then E is λ -distributive for all $\lambda < \kappa$.*

PROOF. Let $\lambda < \kappa$, and let D_ξ , $\xi < \lambda$, be open dense subsets of P . Let $p \in P$ be arbitrary. We attempt to construct $p_\lambda \leq p$ with $p_\lambda \in \bigcap_{\xi < \lambda} D_\xi$, proving density. We do this by attempting to construct a decreasing sequence $p_\xi = \langle E_\xi, \alpha_\xi \rangle$, $\xi \leq \lambda$, as follows:

Let $p_0 = p$. At a successor step, if p_ξ is defined, note that trivially $\langle E_\xi, \alpha_\xi + 1 \rangle \leq p_\xi$. Choose $p_{\xi+1} \leq \langle E_\xi, \alpha_\xi + 1 \rangle$ belonging to D_ξ . This ensures that $\alpha_\xi \notin E_{\xi+1}$. At a limit step, if p_ξ is defined for all $\xi < \zeta$, let $\alpha = \sup\{\alpha_\xi : \xi < \zeta\}$, $E = \bigcup_{\xi < \zeta} E_\xi$. If $\langle E, \alpha \rangle \in P$, set $E_\zeta = E$, $\alpha_\zeta = \alpha$, $p_\zeta = \langle E, \alpha \rangle$. If $\langle E, \alpha \rangle \notin P$, p_ζ is undefined and our inductive construction breaks down.

Clearly p_λ , if defined, belongs to all D_ξ as required. Assume for contradiction that the above process breaks down at some limit $\zeta \leq \lambda$. This can only happen if, in the notation above, $E \cap \beta$ is stationary in β for some limit ordinal $\beta \leq \alpha$. If $\beta < \alpha$, then $\beta < \alpha_\xi$ for some $\xi < \zeta$ and $E \cap \beta = E_\xi \cap \beta$ is not stationary in β . So E must be stationary in α .

By construction, however, E is disjoint from $C = \{\alpha_\xi : \xi < \zeta\}$, since $\alpha_\xi \notin E_{\xi+1}$. Clearly this C is unbounded in α . If $\xi < \eta < \zeta$, then $\alpha_\xi < \alpha_\eta$. Thus if β is a limit point of C , β has the form $\sup\{\alpha_\xi : \xi < \eta\}$ for some limit $\eta < \zeta$. But then by construction $\beta = \alpha_\eta \in C$. Thus C is closed in α . E is disjoint from the CUB set C , hence nonstationary; a contradiction completing the proof. $\square$

4.16. THEOREM (Jensen). *There exists a CTM N with $N \models E(\omega_2)$, and the same is true for $E(\omega_3)$, etc.*

PROOF. Because the notions of CUB and stationary set degenerate in the case of countable ordinals, we do not consider $E(\omega_1)$. Let M be a CTM with $M \models \text{GCH}$. Let $\kappa = \omega_2^M$ or ω_3^M or what have you. Let $P \in M$ be such that $M \models P$ is the $E(\kappa)$ PO set. Let $G \subseteq P$ be M -generic, $N = M[G]$, $E = \bigcup_{p \in G} E_p$. By the distributivity and κ^+ -antichain conditions on P (the latter being trivial, since $\text{card}^M P = \kappa$), all cardinals of M are preserved in N . We show E is as required to make $E(\kappa)$ true inside N .

If $p, q \in P$ are compatible, $E_p = E_q \cap \alpha_p$ or vice versa. Since all elements of G are compatible, it follows $E_p = E \cap \alpha_p$ for all $p \in G$. If $D_\alpha =$

$\{p \in P: \alpha_p > \alpha\}$, then it is quite easily seen that D_α is dense for all $\alpha < \kappa$. Now consider a limit ordinal $\alpha < \kappa$. There is $p \in D_\alpha \cap G$. For such p , $E \cap \alpha = E_p \cap \alpha$. Now $E_p \cap \alpha$ is not stationary in α inside M , i.e. there is a CUB $C \in M$ with $C \cap E_p = \emptyset$. Since this same C is present in N , $E \cap \alpha$ is not stationary in α inside N , either. It thus only remains to show that E is stationary in κ inside N , i.e. for any CUB $C \subseteq \kappa$ belonging to N , $C \cap E \neq \emptyset$. This turns out to be a bit tricky.

Any $C \in \mathcal{P}^N(\kappa)$ has form $I_G(t)$ for some $t \in \mathcal{P}^M(P \times \kappa)$. If C is CUB, some $p_0 \in G$ forces that t is CUB in κ^* . Let $\bar{G} = \{\langle p, p \rangle: p \in P\}$, the canonical term having $I_G(\bar{G}) = G$. It follows that if $p \in P$, $\alpha < \alpha_p$, then $p \Vdash (\alpha^* \in \bigcup \text{range } \bar{G})$ iff $\alpha \in E_p$. (Since for any generic H with $p \in H$, $\alpha \in \bigcup \text{range } I_H(\bar{G}) = \bigcup_{q \in H} E_q$ iff $\alpha \in E_p$.) To prove that $C \cap E \neq \emptyset$, it suffices to show that some $p \in G$ forces

$$(*) \quad t \cap \bigcup \text{range } \bar{G} \neq \emptyset.$$

We show that in fact $p_0 \Vdash (*)$, by showing that the set of $p \leq p_0$ forcing $(*)$ is dense below p_0 . And for this it suffices to find for any $p \leq p_0$ a $q \leq p$ and an α such that $q \Vdash \alpha^* \in t$ and $\alpha \in E_q$.

So let $p \leq p_0$ be arbitrary. All of the following is true inside M : We can define a decreasing sequence $q_n = \langle E_n, \alpha_n \rangle$ in P , and an increasing sequence β_n of ordinals $< \kappa$, for $n < \omega$, as follows: Let $q_0 = p$, $\beta_0 = 0$. If q_n, β_n are defined, then since $q_n \leq p_0$, $q_n \Vdash t$ is unbounded in κ^* . Hence $q_n \Vdash \exists \beta (\alpha_n^* + 1, \beta_n^* < \beta < \kappa^* \wedge \beta \in t)$. We can thus choose $q_{n+1} \leq \langle E_n, \alpha_n + 1 \rangle \leq q_n$ and β_{n+1} with $\alpha_n + 1, \beta_n < \beta_{n+1} < \kappa$ and $q_{n+1} \Vdash \beta_{n+1}^* \in t$. Let $E' = \bigcup_{n < \omega} E_n$, $\gamma = \sup\{\alpha_n: n < \omega\} = \sup\{\beta_n: n < \omega\}$. Then $q = \langle E' \cup \{\gamma\}, \gamma + 1 \rangle$ is $\leq$ all q_n and has $\gamma \in E_q$. Moreover, $q \Vdash t$ is closed in κ^* , and $q \Vdash \beta_n^* \in t$ for all n , so $q \Vdash \gamma^* \in t$. Thus we have found a $q \leq p$ and a $\gamma \in E_q$ such that $q \Vdash \gamma^* \in t$, as required. $\square$

We close this section with a mention of two more principles.

4.17. EXERCISE. If T is an ω_2 Kurepa tree, F a family of branches through T , and $C \subseteq T$ is of cardinality ω_1 , then $\{B \cap C: B \in F\}$ has cardinality $\leq \omega_1$. (Because $C \subseteq T_\alpha$ for some $\alpha < \omega_2$, and $B \cap C$ is then completely determined by the unique $a \in B \cap T_\alpha$, and $\text{card } T_\alpha \leq \omega_1$.) Show that we can get a CTM in which there is an ω_2 Kurepa tree and a family F of ω_3 branches through T such that for any countable $C \subseteq T$, $\{B \cap C: B \in F\}$ is countable. Do this by considering the suborder of the $\text{KH}(\omega_2)$ PO set consisting of those p such that for any countable $C \subseteq T_p$ the family

$\{\{a \in C: a \leq b\}: b \in \alpha_p\text{-th level of } T_p\}$ is countable. Show that this suborder is still ω_1 -closed, etc., then proceed as in Theorem 4.4.

4.18. EXERCISE (more difficult). Let κ be a regular cardinal. $\diamond(\kappa)$ is the proposition that there exists a function S with domain κ such that:

(i) $S(\alpha) \subset \alpha$ for all $\alpha < \kappa$.

(ii) For any $A \subseteq \kappa$, $\{\alpha < \kappa: S_\alpha = A \cap \alpha\}$ is stationary in κ . Let the $\diamond(\kappa)$ PO set be the set of all functions p with domain an ordinal $< \kappa$ and $p(\alpha) \subseteq \alpha$ for all $\alpha \in \text{dom } p$, partially ordered by reverse inclusion.

Show that if M is a CTM with $M \models \text{GCH}$, $\kappa = \omega_1^M$, $M \models P$ is the $\diamond(\kappa)$ PO set, and $G \subseteq P$ is M -generic, $N = M[\bar{G}]$, $S = \bigcup G \in N$, then S is as required to make $\diamond(\omega_1)$ true inside N . Do this by considering terms $t, u \in M$ such that $I_G(t), I_G(u) \subseteq \kappa$ and $I_G(t)$ is CUB. Show how to form inside M sequences $p_n \in P$, $B_n \in M$, $\beta_n < \kappa$ such that $p_n \Vdash \beta_n^* \in t$, $\beta_{n+1} > \text{dom } p_n$, $p_{n+1} \Vdash u \cap \beta_n^* = B_n^*$. (To get this last, note that by closure $\mathcal{P}^M(\beta) = \mathcal{P}^N(\beta)$ for any $\beta < \kappa$. Thus if $v \in \mathcal{P}^M(P \times \beta)$ and $X = \mathcal{P}^M(\beta)$, $p \Vdash v \in X^*$.) Then show any $q \leq$ all p_n will force $\beta^* \in t$ and $\bigcup \bar{G}(\beta^*) = B^*$, where β is the sup of the β_n , B the union of the B_n . The argument parallels the proof of Theorem 4.16.

5. Doing two things at once

Sometimes to construct a model a natural procedure is to start with a CTM, M , a PO set $Q \in M$, an M -generic $M \subseteq Q$, and the Cohen extension $M' = M[H]$, and then take a new PO set $R \in M'$, and an M' -generic $K \subseteq R$, forming the extension $N = M'[K] = M[H][K]$. We employed such a procedure in proving Theorem 4.5. It is also a natural approach to proving the consistency of such combinations as $2^\omega > \omega_1 \wedge 2^{\omega_1} > 2^\omega$. We show that such double forcing can be reduced to single forcing. We consider first the case that $R \in M'$ already belongs to M . In this section it is necessary to distinguish a PO set P from its underlying set $|P|$.

5.1. DEFINITION. Let Q, R be PO sets. The *direct product* $Q \otimes R$ of Q and R is the PO set with underlying set $|P| = |Q| \times |R|$ (Cartesian product) and partial ordering $\langle q, r \rangle \leq_P \langle q', r' \rangle$ iff $q \leq_Q q'$ and $r \leq_R r'$. Note that the maximum element 1_P of P is thus $\langle 1_Q, 1_R \rangle$.

5.2. FIRST PRODUCT THEOREM. Let M be a CTM, $Q, R \in M$ PO sets, and $P = Q \otimes R$. Then:

(i) If G is an M -generic subset of P , and we set

$$H = \{q \in |Q| : \exists r \in |R| (\langle q, r \rangle \in G)\},$$

$$K = \{r \in |R| : \exists q \in |Q| (\langle q, r \rangle \in G)\},$$

then H is an M -generic subset of Q , K is an $M[H]$ -generic subset of R , and $G = H \times K$.

(ii) If H is an M -generic subset of Q , and K an $M[H]$ -generic subset of R , then $H \times K$ is an M -generic subset of P .

(iii) If H is an M -generic subset of Q , and K an $M[H]$ -generic subset of R , then K is also M -generic, and H is $M[K]$ -generic.

PROOF. (i) Note that if $\langle q, r \rangle \in G$, then $\langle 1_Q, r \rangle$ and $\langle q, 1_R \rangle \in G$, since these elements are $\geq_P \langle q, r \rangle$. Thus $H = \{q \in |Q| : \langle q, 1_R \rangle \in G\}$, $K = \{r \in |R| : \langle 1_Q, r \rangle \in G\}$.

To show H M -generic: Consider an arbitrary dense $D \in \mathcal{P}^M(|Q|)$. $D \times |R|$ is dense in P , hence there is $\langle q, r \rangle \in (D \times |R|) \cap G$. Then $q \in D \cap H$, $D \cap H \neq \emptyset$.

To show K $M[H]$ -generic: Consider an arbitrary dense $D \in \mathcal{P}^{M[H]}(|R|)$. $D = I_H(t)$ for some $t \in \mathcal{P}^M(|Q| \times |R|)$, and some $q_0 \in Q$ forces that t is dense. Let $E = \{\langle q, r \rangle : q \leq_Q q_0 \wedge q \Vdash r^* \in t\}$. ($E \in M$ by the Definability Lemma.) We claim E is dense below $\langle q_0, 1_R \rangle$ in P .

For if $\langle q, r \rangle \leq_P \langle q_0, 1_R \rangle$, then $q \Vdash (t \text{ is dense in } R^*)$ so $q \Vdash \exists r' \in |R|^* (r' \leq_R r^* \wedge r' \in t)$. So there exist $q' \leq_Q q$ and $r' \leq_R r$ such that $q' \Vdash (r')^* \in t$. But $\langle q', r' \rangle \leq_P \langle q, r \rangle$ and belongs to E , proving density.

It follows (cf. Lemma 2.13) that there is some $\langle q, r \rangle \in E \cap G$. Thus $r \in K$, and since $q \in H$ forces $r^* \in t$, $r \in D$. Thus $D \cap K \neq \emptyset$ as required to prove K generic.

Finally $H \times K \subseteq G$ since if $q \in H$, $r \in K$, then $p_0 = \langle q, 1_R \rangle$ and $p_1 = \langle 1_Q, r \rangle$ belong to G , so there is $p' = \langle q', r' \rangle \in G$ with $p' \leq_P p_0, p_1$. Clearly $\langle q, r \rangle \geq_P p'$, so $\langle q, r \rangle \in G$ as required. The inclusion $G \subseteq H \times K$ is immediate, completing the proof of (i).

(ii) will not be used below, and its proof is left to the interested reader. (iii) follows from (i), (ii), and the fact that $Q \otimes R$ and $R \otimes Q$ are isomorphic. $\square$

The case of double forcing with $R' \in M' - M$ is more difficult. We can make some simplifying assumptions: (i) We assume $|R|$ is an ordinal ρ . Hence $|R| \in M$, since $\text{OR}^{M'} = \text{OR}^M$. (ii) We assume the maximum element 1_R of R is just the ordinal 1. Any PO set is isomorphic to one satisfying these conditions.

The order relation $\leq_R$ of R has the form $I_H(t)$ for some term $t \in \mathcal{P}^M(|Q| \times \rho \times \rho)$. Moreover, some $q \in H$ forces that t makes ρ^* a PO set with maximum element 1^* . Applying Corollary 2.17, we can get a term $\bar{R}$ such that

(*) $Q \Vdash \bar{R}$ makes ρ^* a PO set with maximum element 1^*

and $q \Vdash t = \bar{R}$, whence $I_H(\bar{R}) = I_H(t)$, i.e., $I_H(\bar{R})$ is the order relation on R . A term satisfying (*) we call *good*.

5.3. DEFINITION. Let M be a CTM, $Q \in M$ a PO set, $\rho \in \text{OR}^M$, $X = P^M(|Q| \times \rho)$, $\bar{R} \in M$ a good term. Let $P_0 = \{\langle q, \bar{r} \rangle \in |Q| \times X : q \Vdash \bar{r} \in \rho^*\}$. For elements of P_0 define $\langle q, \bar{r} \rangle \leq_0 \langle q', \bar{r}' \rangle$ iff $q \leq_Q q'$ and $q \Vdash \bar{r} \leq \bar{r}'$ in $\bar{R}$, i.e. $\langle r, r' \rangle \in \bar{R}$. The relation $\leq_0$ will not in general be antisymmetric, but

(**) $\langle q, \bar{r} \rangle \leq_0 \langle q', \bar{r}' \rangle$ and $\langle q', \bar{r}' \rangle \leq_0 \langle q, \bar{r} \rangle$

is easily seen to define an equivalence relation. In fact (**) amounts to saying that $q = q'$ and $q \Vdash (\bar{r} = \bar{r}')$. Let $[q, \bar{r}]$ be the equivalence class of $\langle q, \bar{r} \rangle$. Let $|P|$ be the set of all such equivalence classes, and define $[q, \bar{r}] \leq_P [q', \bar{r}']$ iff $\langle q, \bar{r} \rangle \leq_0 \langle q', \bar{r}' \rangle$. (This definition is easily seen to be independent of choice of equivalence class representatives.) Then $P = \langle |P|, \leq_P \rangle$ is a PO set with maximum element $1_P = [1_Q, 1^*]$. P is called the *forcing product* of Q and $\bar{R}$ (with respect to M), and we write $P = Q \otimes \bar{R}$.

5.4. SECOND PRODUCT THEOREM. *Let the notation be as in 5.3. Let G be an M -generic subset of P . Set*

$$H = \{q \in |Q| : \exists \bar{r} \in X [q, \bar{r}] \in G\},$$

$$K = \{I_H(\bar{r}) : \exists q \in |Q| ([q, \bar{r}] \in G)\}.$$

Then H is an M -generic subset of Q and K is an $M[H]$ -generic subset of the PO set $R = \langle \rho, I_H(\bar{R}) \rangle$.

PROOF. We leave the proof that H is M -generic to the reader. To show K $M[H]$ -generic, consider an arbitrary dense subset D of R . $D = I_H(t)$ for some $t \in X$, and there is $q_0 \in H$ which forces that t is dense. We claim $E = \{[q, \bar{r}] : q \Vdash \bar{r} \in t\}$ is dense below $[q_0, 1^*]$ in P . For let $[q, \bar{r}] \leq_P [q_0, 1^*]$. Since $q \Vdash t$ is dense, $q \Vdash \exists \sigma \in \rho^* (\sigma < r \text{ in } \bar{R} \wedge \sigma \in t)$. Hence there exist $q' \leq_Q q$ and $\sigma \in \rho$ such that $q' \Vdash \sigma^* \in t$. Thus $[q', \sigma^*] \leq_P [q, \bar{r}]$ and belongs to E , proving density. It follows that there is some $[q, \bar{r}] \in E \cap G$. Then $I_H(\bar{r}) \in K$, and $q \in H$. Since, further, $q \Vdash \bar{r} \in t$, $I_H(\bar{r}) \in D$. Thus $D \cap H \neq \emptyset$ as required. $\square$

Theorem 5.2(ii) reduces double forcing to single forcing. Theorem 5.2(i) enables us to regard a single forcing as a two-stage affair in certain circumstances. The usefulness of this result is illustrated by Theorem 5.7 below. For the rest of this section we can revert to our old abuse of notation, not distinguishing between a PO set and its underlying set. No confusion should result.

5.5. DEFINITION. Let κ be an inaccessible cardinal. The κ -Collapsing PO set is

$$P = \{p : (p \text{ is a function}) \wedge (\text{dom } p \text{ is countable} \wedge \text{dom } p \subseteq \kappa \times \omega_1 \wedge \bigwedge \langle \alpha, \xi \rangle \in \text{dom } p (p(\alpha, \xi) < \alpha))\},$$

partially ordered by reverse inclusion. For $\alpha < \kappa$, let P_α be the suborder of P $\{p \in P : \text{dom } p \subseteq \alpha \times \omega_1\}$, and P^α the suborder $\{p \in P : \text{dom } p \subseteq (\kappa - \alpha) \times \omega_1\}$. Then $P_\alpha \otimes P^\alpha$ and P are isomorphic under the map sending $\langle q, r \rangle$ to $q \cup r$.

5.6. LEMMA. Let κ be an inaccessible cardinal, P the κ -Collapsing PO set. Then P is κ -AC.

PROOF. Let $A \subseteq P$ have cardinality κ . We show A is not an antichain. To do this we define for $\xi < \omega_1$ sets $A_\xi \subseteq A$ with $\text{card } A_\xi < \kappa$, as follows: Let $A_0 = \{a\}$ for some arbitrary $a \in A$. If A_ξ is defined for $\xi < \eta$, let $D_\eta = \bigcup_{\xi < \eta} \bigcup_{p \in A_\xi} \text{dom } p$. By regularity, $\text{card } D_\eta < \kappa$, and $D_\eta \subseteq \alpha \times \omega_1$ for some $\alpha < \kappa$. Thus $B_\eta = \{p \mid D_\eta : p \in A\}$ has $\text{card } B_\eta \leq (\text{card } \alpha)^{\text{card } \alpha} < \kappa$. So we can pick $A_\eta \supseteq \bigcup_{\xi < \eta} A_\xi$ with $A_\eta \in A$ and $\text{card } A_\eta < \kappa$ such that for every $q \in B_\eta$ there is $p \in A_\eta$ with $p \restriction D_\eta = q$. Finally, let A' be the union of the A_ξ , $\xi < \omega_1$, and D the union of the D_ξ . $\text{Card } A' < \kappa$, so there is $p \in A - A'$. $\text{Dom } p$ is countable, so $\text{dom } p \cap D \subseteq D_\xi$ for some $\xi < \omega_1$. Hence for some $q \in A_{\xi+1} \subseteq A'$, $p \restriction (\text{dom } p \cap D) = q \restriction D_\xi$. Since $\text{dom } q \subseteq D$, p and q agree on $\text{dom } p \cap \text{dom } q$. Thus $p \cup q$ is a function extending both p and q , and A is not an antichain. $\square$

Collapsing PO sets were introduced by Lévy and used by him and by Solovay in many impressive results. (See SOLOVAY [1970].) The example given here (Theorem 5.7) is due to SILVER [1971]. Just for this result we assume the existence of a CTM M with $M \models$ there exists an inaccessible cardinal. By methods of Gödel (mentioned above after Theorem 3.14), having one such M we can get one with $M \models \text{GCH}$.

5.7. THEOREM (Silver). *There exists a CTM M with $M \models \neg \text{KH}(\omega_1)$.*

PROOF. We are assuming that there exists a CTM M and a $\kappa \in M$ such that $M \models \kappa$ is an inaccessible cardinal. As remarked, we may take $M \models \text{GCH}$. Let $P \in M$ be such that $M \models P$ is the κ -Collapsing PO set. Let $G \subseteq P$ be M -generic, $N = M[G]$. By the (trivial) countable closure of P inside M and the κ -AC, all cardinals in $M \leq \omega_1^M$ or $\geq \kappa$ are preserved in N . But it is easily seen that for $\alpha < \kappa$,

$$\{ \langle \xi, \beta \rangle : \exists p \in G (\langle \alpha, \xi \rangle \in \text{dom } p \wedge p(\alpha, \xi) = \beta) \} \in N$$

is a surjection from ω_1^M to α . Thus there are no cardinals in N between $\omega_1^M = \omega_1^N$ and κ , i.e. $\kappa = \omega_2^N$.

Any tree of height ω_1 whose levels are all countable is isomorphic to a tree with underlying set $|T| = \omega_1$.

Suppose $T \in M$ is a tree with underlying set ω_1^M . Let F be the set of all branches through T in M . Then $\text{card}^M F \leq \omega_2^M$ and $\text{card}^N F \leq \text{card}^N \omega_2^M = \omega_1^M$. Moreover, by Lemma 4.6, every branch through T in N already belongs to M . So in N , T cannot be a Kurepa tree.

Now suppose more generally $T \in N$ is a tree with underlying set ω_1^M . Let $t \in \mathcal{P}^M(P \times \omega_1^M \times \omega_1^M)$ be such that $I_G(t)$ is the order relation $\leq_T$ of T .

All the following is true inside N : If $\xi \leq_T \eta$, then there is $p \in G$ with $\langle p, \xi, \eta \rangle \in t$. Let $f(\xi, \eta)$ be one such p . If $\xi, \eta < \omega_1^M$ and not $\xi \leq_T \eta$, then there is $p \in G$ such that for no $q \leq p$ do we have $\langle q, \xi, \eta \rangle \in t$. (Viz., any p forcing $\langle \xi^*, \eta^* \rangle \notin t$.) Let $f(\xi, \eta)$ be one such p . By regularity of $\kappa (= \omega_2^N)$, there is $\alpha < \kappa$ such that $\text{dom } f(\xi, \eta) \subseteq \alpha \times \omega_1^M$ for all ξ, η .

Now $P = P_\alpha \times P^\alpha$, and Theorem 5.2 implies that $G_\alpha = G \cap P_\alpha$ is M -generic, and $G^\alpha = G \cap P^\alpha$ is $M[G_\alpha]$ -generic. Moreover $M[G_\alpha][G^\alpha] = M[G] = N$. All the $f(\xi, \eta) \in G_\alpha$, so $\leq_T$ is $I_G(t \cap (P_\alpha \times \omega_1^M \times \omega_1^M))$, and $T \in M[G_\alpha]$.

Let ν be $(\text{card } \alpha)^{++}$ in the sense of M . Since κ is inaccessible inside M , $\nu < \kappa$. It is easily seen that $\text{card}^M P_\alpha < \nu$, so trivially $M \models P$ is ν -AC. Thus all cardinals $\geq \nu$ are preserved in $M[G_\alpha]$. By an easy computation using Theorem 3.15 $M[G_\alpha] \models 2^\mu = \nu$, where $\mu = \omega_1^M$. Hence if F is the set of all branches through T in $M[G_\alpha]$, $\text{card}^{M[G_\alpha]} F \leq \nu < \kappa$, and $\text{card}^N F \leq \omega_1^M$.

Now $M \models P_\alpha$, P^α are ω -closed. By ω -closure for P_α , there are no countable sequences of elements of P^α present in $M[G_\alpha]$ except the ones already present in M . Hence $M[G_\alpha] \models P^\alpha$ is ω -closed. Thus we can apply 4.6 to conclude that any branch through T in $N = M[G_\alpha][G^\alpha]$ was already

present in $M[G_\alpha]$, i.e. belongs to F . Thus T is not a Kurepa tree inside N . Since T was arbitrary, $N \models \neg \text{KH}(\omega_1)$. $\square$

We will soon see that Theorem 5.2, which was designed to let us do two things at once, actually lets us do infinitely many things at once. First a crucial lemma.

5.8. LEMMA. *Let M be a CTM, $Q, R \in \text{MPO}$ sets, $P = Q \otimes R$, κ a cardinal in M . Suppose*

$$M \models (\kappa \text{ is regular} \wedge \forall \lambda < \kappa (Q \text{ is } \lambda\text{-closed}) \wedge R \text{ is } \kappa\text{-AC}).$$

Then $p \Vdash \kappa$ is cardinal.

PROOF. Let $G \subseteq P$ be M -generic. Let $H \subseteq Q$, $K \subseteq R$ be as in 5.2(i). We must show κ is preserved in $M[G] = M[H][K]$. Assume for contradiction that $\lambda < \kappa$ and $f \in M[G]$ is a surjection from λ to κ . $f = I_G(t)$ for some $t \in \mathcal{P}^M(P \times \lambda \times \kappa)$, and some $p_0 = \langle q_0, r_0 \rangle$ forces that t is a surjection from λ^* to κ^* .

All the following is true inside M : For $\beta < \kappa$, $q \leq_Q q_0$, let us say a set $A \subseteq \kappa$ β -supports q if whenever $\langle q', r' \rangle \leq_P \langle q, r_0 \rangle$ and $\alpha < \kappa$ and $q \Vdash t(\beta^*) = \alpha^*$, then $\alpha \in A$. Let $D_\beta = \{q \in Q : \exists A \subseteq \kappa (\text{card } A < \kappa \wedge A \text{ } \beta\text{-supports } q)\}$. We claim each D_β is dense below q_0 .

Still inside M , we prove this claim as follows: Let $q \leq_Q q_0$ be arbitrary. We form, for some $\zeta < \kappa$ to be determined, a decreasing sequence $q_\xi, \xi \leq \zeta$, in Q , and $r_\xi \in R$, $\alpha_\xi < \kappa$, for $0 < \xi < \zeta$, as follows: Let $q_1 = q$, $r_1 = r_0$, $\alpha_1 = 0$. If $\eta < \kappa$ and q_ξ, r_ξ, α_ξ are defined for $0 < \xi < \eta$, then by the closure condition on Q , there is $q' \leq_Q$ all q_ξ . If $\{\alpha_\xi : 0 < \xi < \eta\}$ β -supports q' , then we have found a $q' \leq_Q q$ in D_β , and we may stop, setting $q_\eta = q'$ and $\zeta = \eta$. Otherwise, there exist $\langle q_\eta, r_\eta \rangle \leq_P \langle q', r_0 \rangle$ and $\alpha_\eta < \kappa$ such that $\langle q_\eta, r_\eta \rangle \Vdash t(\beta^*) = \alpha_\eta^*$. (Since $\langle q', r_0 \rangle \Vdash \exists \alpha < \kappa^* (t(\beta^*) = \alpha)$.) Note that for distinct ξ , the $\langle q_\xi, r_\xi \rangle$ thus constructed are incompatible. (They force contradictory things about $t(\beta^*)$.) Since the q_ξ form a descending sequence, the r_ξ must be incompatible. Since R is κ -AC, the construction *must* stop at some stage $\zeta < \kappa$, yielding $q_\zeta \leq_Q q$ in D_β , as required to prove density.

The following is also true inside M : Q is λ -closed, hence λ -distributive. It follows $D = \bigcap_{\beta < \lambda} D_\beta$ is dense below q_0 . For $q \in D$, let $A(q, \beta)$ be for each $\beta < \lambda$, a set of cardinality $< \kappa$ β -supporting q , and let $A(q) = \bigcap_{\beta < \lambda} A(q, \beta)$. $\text{Card } A(q) < \kappa$ by regularity.

All this was true inside M . Now from the density of D below $q_0 \in H$, it

follows there is $q \in D \cap H$. Since $\text{card}^M A(q) < \kappa$, there is $\alpha \in \kappa - A(q)$. Now $\alpha = f(\beta)$ for some $\beta < \lambda$. But then there is $\langle q', r' \rangle \in G$ forcing $t(\beta^*) = \alpha^*$, and we may as usual take it $\leq_P \langle q, r_0 \rangle \in G$. But then $\alpha \in A(q, \beta) \subseteq A(q)$, a contradiction which completes the proof. $\square$

5.9. THEOREM (Easton). *There is a CTM M with $M \models \forall \kappa < \omega_\omega (2^\kappa > \kappa^+)$.*

PROOF. For $n < \omega$, let P_n be

$$\{p: p \text{ is a function} \wedge \text{card dom } p < \omega_n \wedge \\ \text{dom } p \subseteq \omega_{n+2} \times \omega_n \wedge \text{range } p \subseteq \{0, 1\}\},$$

partially ordered by reverse inclusion. Let Q_n be the set of all sequences $\langle p_0, p_1 \cdots p_n \rangle$ with $p_i \in P_i$, partially ordered by setting $\langle p_0 \cdots p_n \rangle \leq \langle q_0 \cdots q_n \rangle$ iff $p_i \leq q_i$ in P_i for all i . Let Q^n be the set of all infinite sequences $\langle p_{n+1}, p_{n+2}, \dots \rangle$ with $p_i \in P_i$, similarly ordered. Assuming GCH, it is not hard to see, using the Lemma 3.6, that each Q_n is ω_{n+1} -AC. Clearly each Q^n is ω_n -closed. Equally clearly $Q_m \otimes Q^n$ and $Q_n \otimes Q^m$ are isomorphic for all m, n . We call $Q_0 \otimes Q^0$ the *Easton PO set*.

Now let M be a CTM with $M \models \text{GHC}$. Let $P \in M$ be such that $M \models P$ is the Easton PO set. Let $G \subseteq P$ be M -generic, $N = M[G]$. The analysis Easton PO set $\cong Q_n \otimes Q^n$, together with Lemma 5.8, shows that every cardinal of M is preserved in N . It is not hard to see (cf. 3.16(iii)) that inside N we get from $G \cap P_n$ a family of ω_{n+2} subsets of ω_n . Thus N is the sort of CTM required to prove the theorem. $\square$

Theorem 5.9 admits of countless refinements. For the last word, see EASTON [1970].

6. Martin's Axiom

Martin's Axiom (MA) is the proposition:

If P is a CCC (i.e. ω_1 -AC) PO set, and F a family of $< 2^\omega$ dense subsets of P , then there exists an F -generic subset G of P . Note that CH implies MA by Proposition 2.3. Many important consequences of CH in fact follow from MA. MA is most interesting, however, when we have $2^\omega > \omega_1$. We will prove here the consistency of MA plus $2^\omega = \omega_2$. Chapter B.6 contains many applications of MA.

We begin by reducing MA to something apparently weaker.

6.1. PROPOSITION. *Suppose that for every CCC PO set P of cardinality $< 2^\omega$ and every family F of $< 2^\omega$ dense subsets of P , there exists an F -generic subset G of P . Then MA holds.*

PROOF. Let P be an arbitrary CCC PO set, F a family of $< 2^\omega$ dense subsets of P . Let $f: P \times P \rightarrow P$ be a function such that for compatible $p, q \in P$, $f(p, q) <_P p$ and $f(p, q) <_P q$. For $D \in F$, let $f_D: P \rightarrow D$ be such that $f_D(p) \leq_P p$ for all p . Let Q be the smallest suborder of P containing 1_P and closed under f and all the f_D . Then $\text{card } Q < 2^\omega$. By closure under f , elements of Q which are compatible in P are still compatible in Q , hence Q is CCC. By closure under the f_D , $D \cap Q$ is dense in Q for all $D \in F$. By assumption, therefore, there exists a $\{D \cap Q: D \in F\}$ -generic $H \subseteq Q$. It is easily seen that $\{p \in P: \exists q \in H(q \leq_P p)\}$ is an F -generic subset of P . Since P, F were arbitrary, this proves MA. $\square$

Let us call a PO set P *normalized* if its underlying set is either ω or ω_1 and its maximum element is the ordinal 1. Clearly every PO set of cardinality $< \omega_2$ is isomorphic to a normalized PO set. Since we will be working extensively with such sets, it becomes necessary again to distinguish sharply between a PO set P and its underlying set $|P|$. Thus " D is a dense subset of P " means literally that $D \subseteq |P|$ and D is dense in the order $\leq_P$.

Let us outline the procedure, taken from SOLOVAY and TENNENBAUM [1971], which we will use to construct a model of MA and $2^\omega = \omega_2$. We saw in Corollary 3.16(i) that there exists a CTM M with $M \models 2^\omega = 2^{\omega_1} = \omega_2$. If M is such, we say $\langle Q, F \rangle \in M$ is a *counterexample to MA in M* if Q is a PO set, $M \models (Q \text{ is normalized and CCC})$, F is a family of dense subsets of Q , $\text{card}^M F \leq \omega_1^M$, and there exists no F -generic subset of Q in M . $M \models \text{MA}$ iff no such counterexample exists. (Cf. Proposition 6.1, Lemma 2.12(iv).)

If $\langle Q, F \rangle \in M$ is a counterexample to MA in M , and H is an M -generic subset of Q , then a fortiori H is F -generic. Thus $\langle Q, F \rangle$ is not a counterexample to MA in $M[H]$. Note that by CCC, M and $M[H]$ have the same cardinals. Thus forcing can destroy one counterexample to MA. But probably in $M[H]$ there are counterexamples left over from M which were not destroyed by adjoining H , and probably also new counterexamples in $M[H] - M$. If $\langle Q', F' \rangle$ is one of these counterexamples in $M[H]$, we can of course take an $M[H]$ -generic subset H' of Q' and form a model $M[H][H']$ in which neither $\langle Q, F \rangle$ nor $\langle Q', F' \rangle$ is a counterexample to MA. This double forcing could even be reduced to single forcing using the Product Theorems. But clearly if we are going to get a model with *no*

counterexamples, we are going to want to adjoin *infinitely* many generic sets. This will require much more sophisticated iteration techniques, to which we now turn. The point of the lemmas below (6.2 and 6.5) is that we can perform elaborate constructions on PO sets without losing CCC. The lemmas come from SOLOVAY and TENNENBAUM [1971].

6.2. LEMMA. *Let M be a CTM, $Q \in M$ a PO set, $\rho \in \text{OR}^M$, $\bar{R} \in \mathcal{P}^M(|Q| \times \rho \times \rho)$ a term such that $Q \Vdash (\bar{R} \text{ makes } \rho^* \text{ a PO set with maximum element } 1^*)$, $P = Q \otimes \bar{R}$. Then if $M \models Q$ is CCC, and $Q \Vdash (\bar{R} \text{ makes } \rho^* \text{ a CCC PO set})$, then $M \models P$ is CCC.*

PROOF. $\bar{R}$ is what we called in Section 5 a *good* term. Let us write κ for ω_1^M . Assume for contradiction that there exists inside M a sequence $[q_\xi, \bar{r}_\xi]$, $\xi < \kappa$, of pairwise incompatible elements in P . For $\xi < \eta < \kappa$, either q_ξ, q_η are incompatible in Q , or else every $q \leq_Q q_\xi, q_\eta$ forces that $\bar{r}_\xi, \bar{r}_\eta$ are incompatible in the order $\bar{R}$. (For if $q \leq_Q q_\xi, q_\eta$ forces $\exists \sigma \in \rho^*$ (σ is below both $\bar{r}_\xi$ and $\bar{r}_\eta$ in $\bar{R}$), then there exist $q' \leq_Q q$ and $\sigma \in \rho$ such that $q' \Vdash (\sigma^*$ is below both $\bar{r}_\xi$ and $\bar{r}_\eta$ in $\bar{R}$), i.e. $[q', \sigma^*] \leq_P$ both $[q_\xi, \bar{r}_\xi]$ and $[q_\eta, \bar{r}_\eta]$, contrary to the incompatibility of these elements.) All of the following is true inside M : We may without loss of generality assume that Q forces (i.e. that 1_Q forces)

(*) $\bar{r}_\xi, \bar{r}_\eta \in \rho^* \rightarrow \bar{r}_\xi, \bar{r}_\eta$ are incompatible in the order $\bar{R}$
whenever $\xi < \eta < \kappa$.

For if not, fix a term $\bar{r}$, e.g. ρ^* , such that $1_Q \Vdash \bar{r} \notin \rho^*$. Let $\bar{r}'_\xi, \xi < \kappa$, be terms such that $q_\xi \Vdash \bar{r}'_\xi = \bar{r}_\xi$ and any q incompatible with q_ξ forces $\bar{r}'_\xi = \bar{r}$. (Corollary 2.17 gives us such $\bar{r}'_\xi$.) We claim Q forces (*) with the $\bar{r}'_\xi$ replacing the $\bar{r}_\xi$. To see this it suffices to show for each pair $\xi < \eta < \kappa$ that the set of q forcing (*) with $\bar{r}'_\xi, \bar{r}'_\eta$ replacing $\bar{r}_\xi, \bar{r}_\eta$ is dense. So let $q \in |Q|$ be arbitrary. There is $q' \leq_Q q$ such that either q' is incompatible with one of q_ξ, q_η , or else $q' \leq_Q q_\xi, q_\eta$. In the former case, $q' \Vdash \bar{r}'_\xi \notin \rho^*$ or $q' \Vdash \bar{r}'_\eta \notin \rho^*$; while in the latter case $q' \Vdash \bar{r}'_\xi = \bar{r}_\xi$ and $\bar{r}'_\eta = \bar{r}_\eta$, whence $q' \Vdash \bar{r}'_\xi, \bar{r}'_\eta$ are incompatible. So in either case we have found $q' \leq_Q q$ forcing (*) with $\bar{r}'_\xi, \bar{r}'_\eta$ replacing $\bar{r}_\xi, \bar{r}_\eta$. So the set of q forcing this is dense, and Q forces it, and we may as well assume Q forces (*).

Still inside M we have: There is a q in Q forcing $\forall \xi < \kappa^* \exists \eta > \xi (\bar{r}_\eta \in \rho^*)$. For assume to the contrary every q forces $\exists \xi < \kappa^* \forall \eta > \xi (\bar{r}_\eta \notin \rho^*)$. Then $D = \{q : \exists \xi < \kappa (q \Vdash \forall \eta > \xi^* (\bar{r}_\eta \notin \rho^*))\}$ is dense (by 2.10(v)). By Zorn's Lemma there is an antichain A in Q maximal with respect to the property $A \subseteq D$. It is easily seen that A is actually a maximal

antichain in Q (by density of D). Let $f: A \rightarrow \kappa$ be a function such that $q \Vdash \forall \eta > (f(q))^* (\bar{r}_\eta \notin \rho^*)$ for all $q \in A$. Since Q is CCC, A is countable. Since κ is regular, $\xi = \sup\{f(q): q \in A\}$ is $< \kappa$. Every $q \in A$ forces $\forall \eta > \xi^* (\bar{r}_\eta \notin \rho^*)$, hence Q forces this (by 2.15(ii)). This contradicts the fact that $q_{\xi+1} \Vdash \bar{r}_{\xi+1} \in \rho^*$. This contradiction shows that there is indeed a q forcing $\forall \xi < \kappa^* \exists \eta > \xi (\bar{r}_\eta \in \rho^*)$.

Since $Q \Vdash (*)$ above and (by CCC for Q) also forces that κ^* is a cardinal, such a q forces that $\{\bar{r}_\eta: \eta < \kappa^* \wedge \bar{r}_\eta \in \rho^*\}$ is an uncountable antichain in $\bar{R}$, contrary to $Q \Vdash (\bar{R} \text{ makes } \rho^* \text{ a CCC PO set})$. This contradiction completes the proof. $\square$

6.3. DEFINITION. Let P be a PO set, Q a suborder of P . A map $h: |P| \rightarrow |Q|$ is a *retraction* of P to Q if

- (i) For all $p \in P$, $p \leq h(p)$.
- (ii) For all $q \in Q$, $q = h(q)$.
- (iii) Whenever $p' \leq p$, then $h(p') \leq h(p)$.
- (iv) Whenever $h(p') \leq h(p)$, then there is $p'' \leq p$ with $h(p'') = h(p')$.
- (v) Whenever $h(p)$ and $q \in Q$ are compatible in Q , then p and q are compatible in P .

It is not necessary to distinguish $\leq_P$ and $\leq_Q$ in stating this definition since Q is a suborder of P .

6.4. COROLLARIES TO DEFINITION 6.3. (i) *The property of being a retraction is absolute.*

(ii) *If h is a retraction of P to Q , and k a retraction of Q to R , then kh is a retraction of P to R .*

(iii) *If there exists a retraction of P to a suborder Q of P , then any $q, q' \in |Q|$ which are compatible in P are compatible in Q .*

(iv) *If M is a CTM, $P \in M$ a PO set of the form $Q \otimes \bar{R}$, then the map $h([q, r]) = [q, 1^*]$ is a retraction of P to a suborder Q' of P isomorphic to Q . This h is called the natural retraction.*

(v) *If M is a CTM, $P, Q \in M$ PO sets, $h \in M$ a retraction of P to Q , then for any M -generic subset G of P , $G \cap |Q|$ is an M -generic subset of Q . Further if $\varphi(x)$ is an absolute formula, and $t \in M$ a Q -term such that $Q \Vdash \varphi(t)$, then $P \Vdash \varphi(t)$.*

PROOF. (i) could have been added to the list 2.12. We leave it to the reader, along with (ii).

(iii) Suppose $p \in |P|$ is $\leq q, q'$. By 6.3(ii) and (iii), $h(p) \in |Q|$ is $\leq q, q'$.

(iv) Q' contains all elements of P of form $[q, 1^*]$ and is isomorphic to Q

under the map sending q to $[q, 1^*]$. We leave verification of 6.3(i)–(iii) to the reader.

To see 6.3(iv): Let $p = [q, \bar{r}]$, $p' = [q', \bar{r}']$, and suppose $h(p') \leq_P h(p)$, i.e. $q' \leq_Q q$. Then $p'' = [q', \bar{r}']$ is defined, $p'' \leq_P p$, $h(p'') = h(p')$.

To see 6.3(v): Let $p = [q, \bar{r}]$, $p' = [q', 1^*]$, so that p' is in Q' . Suppose $h(p) = [q, 1^*]$ and p' are compatible in Q , say $p'' = [q'', 1^*]$ is below both. Then $q'' \leq_Q q, q'$, and $p''' = [q'', \bar{r}]$ is defined and is below both p and p' .

(v) Let G be an M -generic subset of P , and consider an arbitrary dense subset D of Q belonging to M . We claim $E = \{p \in P : h(p) \in D\}$ is dense in P . For let p be any element of P . There is some $q \in D$ with $q \leq h(p)$. By 6.3(iv), there is $p' \leq p$ with $h(p') = h(q) = q$, so $p' \in D$, proving density of E . By genericity of G , there exists $p \in E \cap G$. Then $h(p) \in D$, and since $p \leq h(p)$, $h(p) \in G$. Thus $D \cap G \neq \emptyset$, proving genericity for $G \cap Q$.

Note that trivially any Q -term is also a P -term. Further if G is an M -generic subset of P , $I_G(t) = I_{G \cap Q}(t)$. Thus if $Q \Vdash \varphi(t)$, where φ is absolute, then for any generic subset G of P , $M[G \cap Q] \models \varphi(I_G(t))$, and by absoluteness $\varphi(I_G(t))$ is true and true inside $M[G]$, showing that $P \Vdash \varphi(t)$. $\square$

It will now prove convenient to modify the definition of the forcing product $Q \otimes \bar{R}$ so as to make Q itself (and not the isomorph Q' mentioned in 6.4(iv)) a suborder of $Q \otimes \bar{R}$ and to make the natural retraction a retraction to Q . This can easily be accomplished, by expelling from $Q \otimes \bar{R}$ every element of form $[q, 1^*]$, putting q in its place.

6.5. LEMMA. *Let λ be a limit ordinal. Let $P_\xi, \xi \leq \lambda$, be an increasing sequence of PO sets such that for limits $\eta \leq \lambda$, P_η is the union of the $P_\xi, \xi < \eta$. Let $h_\xi, \xi < \lambda$, be retractions of P_λ to P_ξ such that for $\xi < \eta < \lambda$, $h_\xi = h_\xi h_\eta$. Then if each $P_\xi, \xi < \lambda$, is CCC, so is P_λ .*

PROOF. For the definition of the union of an increasing sequence of PO sets, see Definition 2.1. We leave it to the reader to verify that for $\xi < \eta < \lambda$, the restriction of h_ξ to $|P_\eta|$ is a retraction of P_η to P_ξ .

Assume for contradiction that A is an uncountable antichain in P_λ . For $\xi < \lambda$, P_ξ is CCC, so $A \cap |P_\xi|$, being an antichain, is countable. It follows cf $\lambda > \omega$. We define an increasing sequence $\xi(n)$ of ordinals $< \lambda$ and a sequence $B(n)$ with $B(n) \subseteq P_{\xi(n)}$, for $n < \omega$, as follows: Let $\xi(0) = 0$. Having $\xi(n)$, let $B(n)$ be an antichain in $P_{\xi(n)}$ maximal with respect to the property of being a subset of $\{h_{\xi(n)}(p) : p \in A\}$. Necessarily $B(n)$ is countable. Since P_λ is the union of the $P_\xi, \xi < \lambda$, for each $q \in B(n)$ there is an $\eta(q) < \lambda$ with $q = h_{\xi(n)}(p)$ for some $p \in |P_{\eta(q)}| \cap A$. Since cf $\lambda > \omega$,

there is an ordinal $\xi(n+1) < \lambda$ which is $> \xi(n)$ and $> \eta(q)$ for all $q \in B(n)$.

Now let $\eta = \sup\{\xi(n) : n < \omega\} < \lambda$. As $A \cap |P_\eta|$ is countable, there exists some $p \in A - |P_\eta|$. Let $p' = h_\eta(p)$. Since P_η is the union of the $P_{\xi(n)}$, there is an n with $p' \in |P_{\xi(n)}|$. For ξ with $\xi(n) \leq \xi \leq \eta$, $h_\xi(p) = h_\xi h_\eta(p) = h_\xi(p') = p'$. By maximality of $B(n)$, $p' = h_{\xi(n)}(p)$ is compatible with some $q \in B(n)$. Now q itself has form $h_{\xi(n)}(r)$ for some $r \in A \cap |P_{\xi(n+1)}|$ by construction.

By 6.3(v), since $p' \in |P_{\xi(n)}|$ and $q = h_{\xi(n)}(r)$ are compatible in $P_{\xi(n)}$, p' and r are compatible in $P_{\xi(n+1)}$. Again, since $r \in |P_{\xi(n+1)}|$ and $p' = h_{\xi(n+1)}(p)$ are compatible in $P_{\xi(n+1)}$, r and p are compatible in P_λ . But $r, p \in A$, so A is not an antichain, a contradiction. $\square$

6.6. THEOREM (Martin). *There exists a CTM M with $M \models (MA \wedge 2^\omega = \omega_2)$.*

PROOF. We have already hinted at the idea of the proof. We now give details. Let M be a CTM with $M \models 2^\omega = 2^{\omega_1} = \omega_2$. Write λ for ω_1^M and κ for ω_2^M . Recall the definition (given just after Proposition 6.1) of a normalized PO set.

Inside M all the following is true: If P is a CCC PO set with $\text{card } P \leq \kappa$, then $P \models (\lambda^*, \kappa^* \text{ are cardinals } \wedge 2^{\lambda^*} = \kappa^*)$. (This uses 3.4, 3.15.) Hence $P \models$ (there exist only κ^* normalized PO sets). Hence we may (by 2.16) choose terms $U_0(P), U_1(P)$ such that $U_i(P) \subseteq P \times \kappa \times \gamma \times \gamma$, where $\gamma = \omega$ or λ according as $i = 0$ or 1 , and $P \models (U_i(P) \text{ is a function with domain } \kappa^* \text{ and range the set of all order relations of normalized PO sets with underlying set } \gamma^*)$. Let a, b, c be functions with domain $\kappa - \{0\}$ such that for all $\xi < \kappa$, $a(\xi) < \xi$, $b(\xi) < \kappa$, $c(\xi) = 0$ or 1 , and for all $\alpha, \beta < \kappa$ and $i < 2$, there exists a $\xi < \kappa$ such that $a(\xi) = \alpha$, $b(\xi) = \beta$, $c(\xi) = i$.

Still inside M : Using the functions a, b, c for bookkeeping, and also the functions U_0, U_1 , we try to define an increasing sequence $P_\xi, \xi \leq \kappa$, of PO sets, each of cardinality $\leq \kappa$, and each with maximum element 1. In order to carry out the construction, we construct at the same time retractions h_ξ^η of P_η to P_ξ for $\xi < \eta \leq \kappa$, such that $h_\xi^\zeta = h_\xi^\eta h_\eta^\zeta$ when $\xi < \eta < \zeta \leq \kappa$. Let P_0 be any normalized CCC PO set with underlying set ω , and P_1 any such PO set with underlying set λ . At a successor $\eta + 1$: Suppose everything required is defined up to and including stage η . Consider $\alpha = a(\eta)$, $\beta = b(\eta)$, $i = c(\eta)$, and $\gamma = \omega$ or λ according as $i = 0$ or 1 . Let $u = U_i(P_\alpha)$, and let v be a P_α -term such that $P_\alpha \models v = u(\beta^*)$. Thus $P \models (v \text{ is the order relation of a normalized PO set with underlying set } \gamma^*)$. Note that v is also a P_η -term and P_η forces the same thing about v (by 6.5(v)). Let $\bar{R}_\eta$ be a P_η -term such that $P_\eta \models ((v \text{ is CCC } \wedge \bar{R}_\eta = v) \vee (v \text{ is not CCC } \wedge \bar{R}_\eta \text{ is$

the order relation of P_1^*). So in both cases $P_\eta \Vdash (\bar{R}_\eta$ is a normalized PO set with underlying set γ^*). (Such $\bar{R}_\eta$ exists by Theorem 2.14.) Let $P_{\eta+1} = P_\eta \otimes \bar{R}_\eta$. $P_{\eta+1}$ is thus CCC (by Lemma 6.2). *We will verify below that* $\text{card } P_{\eta+1} \leq \kappa$. Let h be the natural retraction of $P_{\eta+1}$ to P_η . Let $h_\xi^{\eta+1} = h$ for $\xi = \eta$, and $h_\xi^\eta h$ for $\xi < \eta$. At a limit $\zeta \leq \kappa$: Let P_ζ be the union of the P_ξ , $\xi < \zeta$, assuming that these are defined. For $\xi < \zeta$, let h_ξ^ζ be the union of the maps h_ξ^η for $\xi < \eta < \zeta$. It is easily checked that these maps are retractions. The existence of such retractions implies this P_ζ is CCC (by Lemma 6.5), and of course $\text{card } P_\zeta \leq \kappa$.

Still inside M , we carry out the verification that $P_{\eta+1}$ as defined above has cardinality $\leq \kappa$. The argument resembles the proof of Theorem 3.15. Since $\text{card } P_\eta \leq \kappa$, it suffices to show for fixed $q \in P_\eta$ that there are only κ equivalence classes $[q, \bar{r}]$ in $P_\eta \otimes \bar{R}_\eta$. Fix such $[q, \bar{r}]$. For each $\sigma < \gamma$, we can find an antichain $A(\sigma, \bar{r})$ below q in P_η , maximal with respect to the property that every $q' \in A(\sigma, \bar{r})$ either forces $\sigma^* \in \bar{r}$ or forces $\sigma^* \notin \bar{r}$. The usual argument shows that the $A(\sigma, r)$ are actually maximal antichains below q in P . Let $B(\sigma, \bar{r}) = \{q' \in A(\sigma, \bar{r}) : q' \Vdash \sigma^* \in \bar{r}\}$, $C(\sigma, \bar{r}) = A(\sigma, \bar{r}) - B(\sigma, \bar{r})$. Now every antichain is countable, so as we vary $\bar{r}$, we only get $\kappa^\omega = \kappa$ different pairs of sequences $B(\sigma, \bar{r})$, $C(\sigma, \bar{r})$, $\sigma < \gamma$. So it suffices to show that if $B(\sigma, \bar{r}) = B(\sigma, \bar{r}')$ and $C(\sigma, \bar{r}) = C(\sigma, \bar{r}')$ for all $\sigma < \gamma$, then $[q, \bar{r}] = [q, \bar{r}']$, i.e. $q \Vdash \bar{r} = \bar{r}'$. Well, suppose q does *not* force $\bar{r} = \bar{r}'$. Since $q \Vdash r, r' \in \gamma^*$, there must exist $q' \leq q$ in P_η and $\sigma < \gamma$ such that $q' \Vdash (\sigma^* \in \bar{r} \wedge \sigma^* \notin \bar{r}')$ or vice versa, say the former. By maximality there is $q'' \in B(\sigma, \bar{r}) \cup C(\sigma, \bar{r})$ compatible with q' . Clearly $q'' \in B(\sigma, \bar{r})$. But $q'' \notin B(\sigma, \bar{r}')$, equally clearly. So $B(\sigma, \bar{r}) \neq B(\sigma, \bar{r}')$. Thus $[q, \bar{r}]$ is completely determined by the sequences $B(\sigma, \bar{r})$, $C(\sigma, \bar{r})$, $\sigma < \gamma$, completing our verification.

Now all the above was true inside M , so we have constructed a $P = P_\kappa \in M$ such that $M \models P$ is a CCC PO set. Let G be an M -generic subset of P , $N = M[G]$. By CCC, M and N have the same cardinals, and $N \models 2^\omega = 2^\lambda = \kappa$. To show $N \models \text{MA}$, it suffices to show that for any $\langle Q, F \rangle \in N$ such that $N = (Q \text{ is a normalized CCC PO set} \wedge F \text{ is a family of } \leq \lambda \text{ dense subsets of } Q)$ that there is an F -generic subset K of Q belonging to N . (Genericity is absolute by 2.12(iv).) For definiteness, let us take the case that the underlying set of Q is λ rather than ω .

Now for $\xi < \kappa$, $G_\xi = G \cap |P_\xi|$ is an M -generic subset of P_ξ (by 6.5(v)). Let $M_\xi = M[G_\xi]$. Thus $M \subseteq M_\xi \subseteq N$, and M and N and M_ξ have the same cardinals. We begin by showing $\langle Q, F \rangle \in M_\alpha$ for some $\alpha < \kappa$. The proof resembles a step in the proof of Theorem 5.7. Fix $t \in \mathcal{P}^M(P \times \gamma \times \gamma)$ with $I_G(t)$ being the order relation on Q .

All the following is true inside N : If $\sigma, \tau < \lambda$, and $\sigma \leq_O \tau$, then there is a $p \in G$ with $\langle p, \sigma, \tau \rangle \in t$. Let $f(\sigma, \tau)$ be one such p . If on the other hand we do not have $\sigma \leq_O \tau$, then there is $p \in G$ such that for no $q \leq_F p$ is $\langle q, \sigma, \tau \rangle \in t$ (viz., a p forcing $\langle \sigma^*, \tau^* \rangle \notin t$). Since $\kappa > \lambda$ is regular, all $f(\sigma, \tau)$ belong to G_α for some $\alpha < \kappa$.

All this was true inside N , showing that the order relation of Q equals $I_{G_\alpha}(t) \in M_\alpha$ for some $\alpha < \kappa$, hence $Q \in M_\alpha$. To handle F , we fix a surjection $f \in N$ from λ to F , and apply a similar argument to $E = \{\langle \sigma, \tau \rangle \in \lambda \times \lambda : \sigma \in f(\tau)\}$, to show that E and hence F belongs to M_α for some $\alpha < \kappa$. Finally, fix a single $\alpha < \kappa$ such that $\langle Q, F \rangle \in M_\alpha$.

Now Q is, in M_α , a normalized PO set with underlying set λ . If $u = U_1(P_\alpha)$ is the term such that $I_{G_\alpha}(u)$ is a surjection from κ onto the set of all order relations of such PO sets, then the order relation of Q is $(I_{G_\alpha}(u))(\beta)$ for some $\beta < \kappa$. Let v be the P_α -term with $P_\alpha \Vdash v = u(\beta^*)$, so $I_{G_\alpha}(v)$ is the order relation of Q . Take $\eta < \kappa$ with $a(\eta) = \alpha$, $b(\eta) = \beta$, $c(\eta) = 1$. Since there are no uncountable antichains in Q inside N , a fortiori there are none inside M_η . Now in the construction of $P_{\eta+1}$ given above, $\bar{R}_\eta$ was a term so chosen that for any M -generic subset H of P_η we would have $I_H(\bar{R}_\eta) = I_H(v)$ if the latter is CCC inside $M[H]$, and is something else otherwise. So in our particular case, $I_{G_\eta}(\bar{R}_\eta) = I_{G_\eta}(v) = I_{G_\alpha}(v)$ is the order relation on Q .

Finally, consider the M -generic subset $G_{\eta+1}$ of $P_{\eta+1} = P_\eta \otimes \bar{R}_\eta$. By Theorem 5.4,

$$K = \{I_{G_\eta}(r) : \exists q \in G_\eta (\langle q, r \rangle \in G_{\eta+1})\} \in M_{\eta+1} \subseteq N$$

is an M_η -generic subset of the PO set with order relation $I_{G_\eta}(\bar{R}_\eta)$, i.e. of Q . Since $F \subseteq M_\alpha \subseteq M_\eta$, K is a fortiori F -generic, and our proof is complete. $\square$

Simple variants of the above argument give models with MA and $2^\omega = \omega_3$, etc.

SOLOVAY [1966] initiated the use of forcing to prove ordinary mathematical theorems (rather than consistency results). Unfortunately we lack space to enter into a discussion of his methods here.

References

- COHEN, P.J.
 [1966] *Set Theory and the Continuum Hypothesis* (Benjamin, New York).
 EASTON, W.B.
 [1970] Powers of regular cardinals, *Ann. Math. Logic*, 1, 139–178.

GÖDEL, K.

- [1940] *The Consistency of the Continuum Hypothesis*, Ann. Math. Studies, Vol. 3 (Princeton Univ. Press, Princeton, NJ).

HALMOS, P.R.

- [1960] *Naive Set Theory* (Van Nostrand, New York).

JECH, T.J.

- [1971] Trees, *J. Symbolic Logic*, **36**, 1–14.

LÉVY, A.

- [1965] A hierarchy of formulas in set theory, *Mem. Am. Math. Soc.*, **57**.

MARCZEWSKI, E.

- [1947] Séparabilité et multiplication cartésienne des espaces topologiques, *Fund. Math.*, **34**, 127–143.

SCOTT, D.S., editor

- [1971] *Axiomatic Set Theory*, Vol. 1, Proceedings of Symposia in Pure Mathematics, Vol. 13 (Am. Math. Soc., Providence, RI).

SHOENFIELD, J.R.

- [1971] Unramified forcing, in: SCOTT [1971] pp. 357–381.

SILVER, J.H.

- [1971] The independence of Kurepa's conjecture and the two-cardinal conjectures in model theory, in: SCOTT [1971] pp. 383–395.

SKOLEM, TH.

- [1922] Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre, in: *Proceedings of the Fifth Scandinavian Mathematical Congress, Helsinki*, pp. 217–232. [English translation in: VAN HEIJENOORT [1967] pp. 290–301.]

SOLOVAY, R.M.

- [1966] The cardinality of Σ_2^1 sets, in: *Foundations of Mathematics: Symposium papers commemorating the sixtieth birthday of Kurt Gödel*, edited by J.J. Bulloff et al. (Springer, Berlin).
- [1970] A model of set theory in which every set of reals is Lebesgue measurable, *Ann. Math.*, **92**, 1–56.

SOLOVAY, R.M. and TENNENBAUM, S.

- [1970] Iterated Cohen extensions and Souslin's problem, *Ann. Math.*, **94**, 201–245.

VAN HEIJENOORT, J., editor

- [1967] *From Frege to Gödel* (Harvard Univ. Press, Cambridge, Mass.)

Constructibility

KEITH J. DEVLIN

Contents

1. Introduction	454
2. The constructible universe	455
3. Arithmetisation of $\mathcal{L}_V$	457
4. The structure of the constructible hierarchy.	460
5. The axiom of constructibility	462
6. The axiom of choice in L	463
7. The condensation lemma. The GCH in L	465
8. Σ_1 Skolem functions	466
9. Admissible ordinals	470
10. The Souslin hypothesis	472
11. The generalised Souslin hypothesis	473
12. The fine structure of the constructible hierarchy	476
13. The combinatorial principle $\square_\kappa$	479
14. Weakly compact cardinals in L	483
15. Other results	487
Historical note.	488
References	489

1. Introduction

The notion of constructibility in set theory was first introduced in GÖDEL [1938], and was used to establish the non-refutability (in ZF — Zermelo–Fraenkel set theory without the axiom of choice — and in ZFC — Zermelo–Fraenkel set theory — respectively) of the axiom of choice and the generalised continuum hypothesis (GCH). The motivation for the definition of “constructibility” is roughly as follows. We are working in ZF. The universe, V , of all sets is “obtainable” by commencing with the null set, $\emptyset$, and iterating the power set operation. In this way we obtain the familiar cumulative hierarchy:

$$V_0 = \emptyset;$$

$$V_\alpha = \bigcup \{ \mathcal{P}(V_\beta) \mid \beta < \alpha \}.$$

And we have

$$V = \bigcup_{\alpha \in \text{On}} V_\alpha,$$

where On is the class of all ordinals. (We use here the usual notations and conventions of set theory, so, in particular, an ordinal number is equal to the set of all smaller ordinal numbers, and a cardinal number is a special kind of ordinal number.)

The reason why certain questions about the cumulative hierarchy are not answerable in ZF or ZFC, so the argument runs, is that the notion of the power set of an infinite set is too vague; we know that $\mathcal{P}(x)$, the power set of x , consists of *all* subsets of x — but what does *all* mean here? The axioms of ZF and ZFC do not help us much. The *constructible universe* is obtained when this looseness is removed by taking the power set of any set as small as possible, without contradicting the ZF axioms. More precisely, we notice that any subset of a given set which is first-order definable (in the language of set theory, $\mathcal{L}$) from other given sets must “exist” (in any “universe”) if the given sets “exist”, and define the constructible hierarchy (with the constructible universe as its limit) by taking, at stage α , not *all* (?) subsets of what we have so far, but only those subsets which are first-order definable from what we have so far. This *minimality* of the constructible universe has the result that for any cardinal κ , 2^κ is as small as possible (hence the GCH holds in the constructible universe). And because every constructible set can be, in a certain sense, uniquely “named” in terms of previously introduced sets, the axiom of choice also holds in the constructible universe.

2. The constructible universe

Let X be any set. By $\text{Def}(X)$ we mean the set of all subsets a of X which are first-order definable over the structure $\langle X, \in, (x)_{x \in X} \rangle$. (See Section 3 of Chapter A.1.) More precisely, for any set X , $\mathcal{L}_X$ denotes the language obtained from $\mathcal{L}$ by introducing a new individual constant $\hat{x}$, to denote x in the structure $\langle X, \in \rangle$, for each $x \in X$, and $\models_X$ denotes the satisfaction relation for $\mathcal{L}_X$ -sentences in the structure $\langle X, \in \rangle$ (with the standard interpretation of the constants), whence $\text{Def}(X)$ is the set of all $a \subseteq X$ such that for some formula $\varphi(v_0)$ of $\mathcal{L}_X$, with free variable v_0 only, $a = \{x \in X \mid \models_X \varphi(\hat{x})\}$.

By recursion on the ordinals, we define the *constructible hierarchy* as follows:

$$L_0 = \emptyset;$$

$$L_{\alpha+1} = \text{Def}(L_\alpha);$$

$$L_\lambda = \bigcup_{\alpha < \lambda} L_\alpha, \text{ if } \lim(\lambda)$$

(i.e. if λ is a limit ordinal). (To see that this really is parallel to the definition of the cumulative hierarchy, notice that $V_{\alpha+1} = \mathcal{P}(V_\alpha)$ for all α and that $V_\lambda = \bigcup_{\alpha < \lambda} V_\alpha$ if $\lim(\lambda)$.)

The *constructible universe* is the class $L = \bigcup_{\alpha \in \text{On}} L_\alpha$. A set x is *constructible* if $x \in L$ (i.e. if there is an α such that $x \in L_\alpha$).

The following lemma is almost immediate from the definitions.

- 2.1. LEMMA.** (i) $\alpha < \beta$ implies $L_\alpha \cup \{L_\alpha\} \subseteq L_\beta$;
 (ii) Each L_α is transitive. L is transitive.
 (iii) For all α , $L \cap \alpha = L_\alpha \cap \alpha = \alpha$ and $\alpha \in L_{\alpha+1}$. $\text{On} \subseteq L$.

As hinted at in our introductory discussion, L is a suitable “universe” for set theory; i.e. L is an inner model of ZF. (An *inner model* of a theory T is a transitive class M such that $\text{On} \subseteq M$ and for each axiom φ of T , φ^M , the relativisation of φ to M , is valid.)

2.2. THEOREM (Gödel). For each axiom φ of ZF, $\text{ZF} \vdash \varphi^L$.

PROOF. (In ZF) *Extensionality*. We must show that $\forall x \forall y [\forall z (z \in x \leftrightarrow z \in y) \leftrightarrow x = y]$ holds in L ; i.e. that for any x, y in L , $x = y \leftrightarrow \forall z \in L (z \in x \leftrightarrow z \in y)$. But L is transitive, so this is valid by the axiom of extensionality in V .

Pairing. Given x, y in L we must show that there is a set z in L whose only members are x and y . But if α is such that $x, y \in L_\alpha$, then $\{x, y\} = \{z \in L_\alpha \mid \models_{L_\alpha} z = \hat{x} \vee z = \hat{y}\} \in \text{Def}(L_\alpha) = L_{\alpha+1} \subseteq L$, so we are done.

Union. Let $x \in L$. We show that $\cup x \in L$. Pick α with $x \in L_\alpha$. Since L_α is transitive, $y = \cup x \subseteq L_\alpha$. But the formula $\varphi(v_0) \equiv \exists v_1 (v_0 \in v_1 \wedge v_1 \in \hat{x})$ defines y as a subset of L_α over L_α , so $y \in \text{Def}(L_\alpha) = L_{\alpha+1} \subseteq L$, as required.

Infinity. By 2.1(iii) $\omega \in L_{\omega+1} \subseteq L$, so this is immediate.

Power Set. Let $x \in L$. Set $y = \{z \in \mathcal{P}(x) \mid z \in L\}$, a bona fide set by the axioms of power set and comprehension in V . For each $z \in y$, let $f(z)$ be the least α such that $z \in L_\alpha$. By the axiom of replacement in V , we can find an α which exceeds all $f(z)$ for $z \in y$. Thus $y \subseteq L_\alpha$. The formula $\varphi(v_0) \equiv \forall v_1 (v_1 \in v_0 \leftrightarrow v_1 \subseteq \hat{x})$ defines y as a subset of L_α over L_α , so $y \in L_{\alpha+1} \subseteq L$. And clearly, $[y = \mathcal{P}(x)]^L$.

Foundation. Since the membership relation of L is just the restriction to L of the usual membership relation, this follows immediately from the axiom of foundation in V .

Comprehension. Let $\varphi(v_0, \dots, v_n)$ be a given $\mathcal{L}$ -formula, $x, a_1, \dots, a_n$ given elements of L . We must show that there is $y \in L$ such that $[y = \{z \in x \mid \varphi(z, a)\}]^L$. Pick α with $x, a \in L_\alpha$. By repeating for the constructible hierarchy the well-known proof of the Reflection Principle, we can find $\beta > \alpha$ such that $\forall z \in L_\beta [\varphi^{L_\beta}(z) \leftrightarrow \varphi^L(z)]$. Let $y = \{z \in x \mid \varphi^L(z, a)\}$. Since $x, a \in L_\beta$ and $y \subseteq x \subseteq L_\beta$, the choice of β ensures that the formula $\psi(v_0) \equiv v_0 \in \hat{x} \wedge \varphi(v_0, a)$ defines y over L_β , so $y \in L_{\beta+1}$, and we are done.

Replacement. Suppose φ is an $\mathcal{L}$ -formula and $a \in L$ and $[\forall x \exists y \varphi(y, x, a)]^L$. Let $u \in L$ be given. We seek a $v \in L$ such that $[\forall x \in u \exists y \in v \varphi(y, x, a)]^L$. Pick α with $u, a \in L_\alpha$. For each $x \in u$, let $f(x)$ be the least $\beta \geq \alpha$ such that $\varphi^L(y, x, a)$ for some $y \in L_\beta$. Let γ exceed all $f(x)$, $x \in u$. Then $v = L_\gamma$ is as required.

The proof is complete. $\square$

In order to prove that AC and GCH hold in L , we must first examine the definition of the constructible hierarchy in some detail. To do this we must first give a set-theoretical definition of the language $\mathcal{L}_V$, and investigate the basic semantic notions of this language.¹

¹ To be precise, in order for the discussion in Section 2 to make sense we needed to know that the language $\mathcal{L}_V$ and its syntax and semantics were formalisable within set theory itself, but since we only needed to know that this is possible, not how it may be done, we did not emphasize this at the time.

3. Arithmetisation of $\mathcal{L}_V$

The following will amount to a formal definition of the language $\mathcal{L}_V$ within set theory. If s and t are finite sequences, $s^\frown t$ denotes the concatenation of s and t (i.e. the finite sequence which starts with s and ends with t).

Variables:

$$v_n \equiv \langle 2, n \rangle, \quad n \in \omega.$$

That is, v_n is the ordered pair $\langle 2, n \rangle$. Let Vbl be the predicate "... is a variable".

Constants:

$$\dot{x} \equiv \langle 3, x \rangle, \quad x \in V.$$

Let $Const$ be the predicate "... is a constant".

Primitive formulas:

$$(x \in y) \equiv \langle 0 \rangle^\frown \langle 4 \rangle^\frown \langle x \rangle^\frown \langle y \rangle^\frown \langle 1 \rangle, \quad \text{where } x, y \in Vbl \cup Const.$$

$$(x = y) \equiv \langle 0 \rangle^\frown \langle 5 \rangle^\frown \langle x \rangle^\frown \langle y \rangle^\frown \langle 1 \rangle, \quad \text{where } x, y \in Vbl \cup Const.$$

Let $PFml$ be the predicate "... is a primitive formula".

Formulas:

$$(\varphi \wedge \psi) \equiv \langle 0 \rangle^\frown \langle 6 \rangle^\frown \varphi^\frown \psi^\frown \langle 1 \rangle$$

$$(\neg \varphi) \equiv \langle 0 \rangle^\frown \langle 7 \rangle^\frown \varphi^\frown \langle 1 \rangle$$

$$(\exists u \varphi) \equiv \langle 0 \rangle^\frown \langle 8 \rangle^\frown \langle u \rangle^\frown \varphi^\frown \langle 1 \rangle, \quad \text{where } Vbl(u).$$

(We are here simply giving schemas for the generation of the formulas from the primitive formulas, of course.)

Let Fml be the predicate "... is a formula". If u is a given set, we define $Const_u(x)$ to be $Const(x) \wedge (x)_1 \in u$ (i.e. x is a constant whose standard interpretation lies in u), and obtain the relativised predicates $PFml_u(x)$ and $Fml_u(x)$ in the obvious way. (Thus, if $Fml_u(x)$, then x is a formula of $\mathcal{L}_u$.) We regard each of these as predicates of both u and x .

The predicates introduced above have the following set-theoretical definitions.

$$Vbl(x) \leftrightarrow [x \text{ is an ordered pair}] \wedge [(x)_0 = 2] \wedge [(x)_1 \text{ is a natural number}];$$

$$Const(x) \leftrightarrow [x \text{ is an ordered pair}] \wedge [(x)_0 = 3];$$

$$\begin{aligned}
\text{PFml}(x) \leftrightarrow & [x \text{ is a sequence}] \wedge [\text{dom}(x) = 5] \wedge [x(0) = 0] \wedge \\
& [x(1) = 4 \vee x(1) = 5] \wedge \\
& [\text{Vbl}(x(2)) \vee \text{Const}(x(2))] \wedge \\
& [\text{Vbl}(x(3)) \vee \text{Const}(x(3))] \wedge \\
& [x(4) = 1]; \\
\text{Fml}(x) \leftrightarrow & \exists f (\text{Build}(x, f)),
\end{aligned}$$

where Build is the predicate:

$$\begin{aligned}
\text{Build}(\varphi, \psi) \leftrightarrow & [\psi \text{ is a finite sequence}] \wedge \psi_{\text{dom}(\psi)-1} = \varphi \wedge \\
& \forall i \in \text{dom}(\psi) (\text{PFml}(\psi_i) \vee \exists j, k \in i (\psi_i = \psi_j \wedge \psi_k) \vee \\
& \exists j \in i (\psi_i = \neg \psi_j) \vee \\
& \exists j \in i \exists u \in \text{ran}(\varphi) (\text{Vbl}(u) \wedge \psi_i = \exists u \psi_j)).
\end{aligned}$$

The predicates $\text{Const}_u(x)$, $\text{PFml}_u(x)$, $\text{Fml}_u(x)$ have similar definitions.

We may now give set-theoretical definitions of the basic syntactical and semantical notions of $\mathcal{L}_v$.

Let $\text{Fr}(\varphi)$ be the set of variables occurring free in φ , if $\text{Fml}(\varphi)$, otherwise let $\text{Fr}(\varphi) = \emptyset$. The function Fr has the set-theoretical definition:

$$\begin{aligned}
y = \text{Fr}(\varphi) \leftrightarrow \\
\leftrightarrow & [\neg \text{Fml}(\varphi) \wedge y = \emptyset] \vee \exists f \exists \psi [\text{Build}(\varphi, \psi) \wedge (f \text{ is a finite} \\
& \text{sequence}) \wedge \text{dom}(f) = \text{dom}(\psi) \wedge f(\text{dom}(f) - 1) = y \wedge \forall i \in \text{dom}(f) \\
& [(\text{PFml}(\psi_i) \wedge f(i) = F(\psi_i)) \vee \exists j, k \in i (\psi_i = \psi_j \wedge \psi_k \text{ and } f(i) = \\
& f(j) \cup f(k)) \vee \exists j \in i (\psi_i = \neg \psi_j \text{ and } f(i) = f(j)) \vee \exists j \in i \exists u \in \\
& \text{ran}(\varphi) (\text{Vbl}(u) \text{ and } \psi_i = \exists u \psi_j \text{ and } f(i) = f(j) - \{u\})]],
\end{aligned}$$

where $F = \text{Fr} \upharpoonright \text{PFml}$. (The function F clearly has a very simple definition, which we omit for brevity.)

If φ is a formula, v is a variable, and t is a constant, $\varphi(v/t)$ denotes the formula obtained from φ by substituting t for every free occurrence of v in φ . We define the function Sub by:

$$\text{Sub}(\varphi, v, t) = \begin{cases} \varphi(v/t), & \text{if } \text{Fml}(\varphi) \wedge \text{Vbl}(v) \wedge \text{Const}(t), \\ \emptyset, & \text{otherwise.} \end{cases}$$

The function Sub has the set -theoretical definition:

$$\varphi' = \text{Sub}(\varphi, v, t) \leftrightarrow$$

$$\begin{aligned} \leftrightarrow & [\neg (\text{Fml}(\varphi) \wedge \text{Vbl}(v) \wedge \text{Const}(t)) \wedge \varphi' = \emptyset] \vee [\text{Fml}(\varphi) \wedge \\ & \text{Vbl}(v) \wedge \text{Const}(t) \wedge \exists \theta \exists \psi [\text{Build}(\varphi, \psi) \wedge \theta \text{ is a finite sequence} \wedge \\ & \text{dom}(\theta) = \text{dom}(\psi) \wedge \theta_{\text{dom}(\theta)-1} = \varphi' \wedge \forall i \in \text{dom}(\psi) \\ & [(\text{PFml}(\psi_i) \wedge \theta_i = S(\psi_i, v, t)) \vee \exists j, k \in i (\psi_i = \psi_j \wedge \psi_k \text{ and } \\ & \theta_i = \theta_j \wedge \theta_k) \vee \exists j \in i (\psi_i = \neg \psi_j \text{ and } \theta_j = \neg \theta_j) \vee \exists j \in i \\ & \exists u \in \text{ran}(\varphi) (\text{Vbl}(u) \text{ and } u \neq v \text{ and } \psi_i = \exists u \psi_j \text{ and } \theta_i = \\ & \exists u \theta_j) \vee \exists j \in i (\psi_i = \exists v \psi_j \text{ and } \theta_i = \psi_i)]]], \end{aligned}$$

where $S = \text{Sub} \upharpoonright (\text{PFml} \times V \times V)$.

Let $\text{Sat}(u, \varphi)$ be the predicate “ φ is a sentence of $\mathcal{L}_u$ such that $\models_u \varphi$ ”. This has the following set-theoretical definition:

$$\text{Sat}(u, \varphi) \leftrightarrow$$

$$\begin{aligned} & u \neq \emptyset \wedge \text{Fml}_u(\varphi) \wedge \exists f \exists \sigma [(f \text{ is a finite sequence}) \\ & \wedge [\varphi \in f(\text{dom}(f) - 1)] \wedge \sigma \subseteq \tau = \\ & [\{v_i = v_j \mid i, j \in \omega\} \cup \{v_i \in v_j \mid i, j \in \omega\} \\ & \cup \{v_i = \hat{x} \mid i \in \omega \wedge x \in u\} \cup \{\hat{x} = v_i \mid i \in \omega \wedge x \in u\} \\ & \cup \{v_i \in \hat{x} \mid i \in \omega \wedge x \in u\} \cup \{\hat{x} \in v_i \mid i \in \omega \wedge x \in u\} \\ & \cup \{\hat{x} \in \hat{y} \mid x, y \in u\} \cup \{\hat{x} = \hat{y} \mid x, y \in u\}]] \\ & \wedge \forall g [(g \text{ is a finite sequence}) \wedge (\text{dom}(g) = \text{dom}(f)) \\ & \wedge (\sigma \subseteq \text{dom}(g) \subseteq \tau) \wedge \forall i \in (\text{dom}(g) - 1) [g(i+1) = \\ & g(i) \cup \{\psi \wedge \psi' \mid \psi, \psi' \in g(i)\} \cup \{\neg \psi \mid \psi \in g(i)\} \\ & \cup \{\exists v_m \psi \mid m \in \omega \wedge \psi \in g(i)\}]] \rightarrow \\ & [f(0) \subseteq \{\hat{x} \in \hat{y} \mid x, y \in u \wedge x \in y\} \cup \{\hat{x} = \hat{x} \mid x \in u\} \wedge \\ & \forall i \in (\text{dom}(f) - 1) [f(i+1) \subseteq f(i) \cup \{\psi \wedge \psi' \mid \psi, \psi' \in f(i)\} \cup \\ & \{\neg \psi \mid \psi \in g(i) - f(i)\} \cup \{\exists v_m \psi \mid m \in \omega \wedge \psi \in g(i) \wedge \\ & \exists x \in u (\text{Sub}(\psi, v_m, \hat{x}) \in f(i))]]]. \end{aligned}$$

The function Def thus has the set-theoretical definition:

$$v = \text{Def}(u) \leftrightarrow$$

$$\begin{aligned} &\leftrightarrow \forall x \in v \exists \varphi [\text{Fml}_u(\varphi) \wedge \text{Fr}(\varphi) = \{v_0\} \wedge x = \{z \in u \mid \\ &\quad \text{Sat}(u, \text{Sub}(\varphi, v_0, z))\}] \wedge \forall \varphi [\text{Fml}_u(\varphi) \wedge \text{Fr}(\varphi) = \{v_0\} \rightarrow \\ &\quad \exists x \in v (x = \{z \in u \mid \text{Sat}(u, \text{Sub}(\varphi, v_0, z))\})]. \end{aligned}$$

4. The structure of the constructible hierarchy

Most of the fundamental lemmas concerning the constructible hierarchy are consequences of one result, to be proved in this section. First, we must remind the reader of some standard notions from logic.

A formula φ of $\mathcal{L}_V$ is said to be Σ_0 if it contains no unbounded quantifiers. (See 1.2 in Chapter B.4, except that there they are called Δ_0 formulas.) It is Σ_n (resp. Π_n) (for $n \geq 1$) if it is of the form $\exists x_1 \forall x_2 \exists x_3 \cdots - x_n \psi$ (resp. $\forall x_1 \exists x_2 \forall x_3 \cdots - x_n \psi$) where ψ is Σ_0 .

A class U is Σ_n^{ZF} if it is defined (over ZF) by a Σ_n formula of $\mathcal{L}$. Similarly Π_n^{ZF} . A class is Δ_n^{ZF} if it is both Σ_n^{ZF} and Π_n^{ZF} .

Let M be a given class, $N \subseteq M$. A predicate (finitary) P on M is $\Sigma_n^M(N)$ if it is defined (over M) by a Σ_n formula of $\mathcal{L}_N$. Similarly $\Pi_n^M(N)$ and $\Delta_n^M(N)$. We write Σ_n^M in place of $\Sigma_n^M(\emptyset)$ and $\Sigma_n(M)$ in place of $\Sigma_n^M(M)$, etc. (Thus, in a certain sense, Σ_n^{ZF} corresponds to " Σ_n^V ".)

These notions have a close connection with the notion of absoluteness, an important concept in constructibility theory.

A predicate P is said to be *absolute* for a class M if for all $x \in M$, $P(x) \leftrightarrow P^M(x)$ (i.e. if P is the same whether interpreted in M or in V).

If M is transitive, any Σ_0 formula of $\mathcal{L}_M$ will be absolute for M , as is easily seen. (Proof by induction on formulas.) It follows immediately that if P is a Δ_1^{ZF} predicate and if M is a transitive model of ZF, or at least of a fragment of ZF which is sufficiently strong to prove the equivalence of the Σ_1 and Π_1 definitions of P , then P is absolute for M .

Most of the basic concepts of set theory are Σ_0^{ZF} , and in fact Σ_0^M for any transitive set M . In particular, are: $x = y$, $x \in y$, $x \subseteq y$, $y = \{x, z\}$, $y = \langle x, z \rangle$, $y = (x)_0$, $y = (x)_1$, $y = \bigcup x$, $y = \bigcap x$, x is an ordered pair, $y = x \times z$, $y = x - z$, x is a function, $y = \text{dom}(x)$, $y = \text{ran}(x)$, $y = x(z)$, $\text{On}(x)$, $\text{lim}(x)$, $\text{succ}(x)$, x is a natural number, x is a sequence, x is a finite sequence, $x = \omega$, $\omega \in x$. In fact, each of these predicates is *uniformly* Σ_0^M for transitive M , which is to say the Σ_0 formula involved in each case is independent of the actual choice of M .

Notice also that if $P(x)$ is Σ_0^{ZF} or else Σ_0^M , where M is transitive, then $P((x)_0)$ and $P((x)_1)$ are also Σ_0 , whence so also are $\forall x \in \text{dom}(u)(P(x))$ and $\forall x \in \text{ran}(u)(P(x))$ (for u a finite sequence, say).

One final comment which we should perhaps make here is that if M is transitive and closed under the formation of ordered pairs, then any Σ_n^M predicate Q on M is expressible in the form $\exists x_1 \forall x_2 \exists x_3 \cdots - x_n R(x_1, \dots, x_n)$, where R is Σ_0^M . (Contraction of quantifiers.)

A function is called Σ_1 just in case its graph is Σ_1 . We now have the necessary prerequisites for:

4.1. LEMMA. *The function $\langle L_\nu \mid \nu \in \text{On} \rangle$ is Σ_1^{ZF} and uniformly Σ_1^* for limit $\lambda > \omega$.*

PROOF. We clearly have:

$$\begin{aligned} y = L_\alpha &\leftrightarrow \\ \leftrightarrow \exists f \Big[&f \text{ is a function} \wedge \text{dom}(f) = \alpha + 1 \wedge f(0) = \emptyset \wedge \\ &\forall \gamma \in \text{dom}(f) \left[\left(\lim(\gamma) \wedge \gamma > 0 \rightarrow f(\gamma) = \bigcup_{\delta < \gamma} f(\delta) \right) \wedge \right. \\ &\left. (\text{succ}(\gamma) \rightarrow f(\gamma) = \text{Def}(f(\gamma - 1))) \right] \wedge y = f(\alpha) \Big]. \end{aligned}$$

We must show that this is Σ_1 by a definition which works both for ZF and arbitrary limit L_λ above ω . Well, by checking through the definitions given in Section 3, it is easily seen that the predicates $\text{Vbl}(x)$, $\text{Const}_u(x)$, $\text{PFml}_u(x)$ are Σ_0 , and that in all the remaining cases, any unbounded quantifiers may, in fact, be bound here by one of:

$$\begin{aligned} \omega, \quad \mathcal{P}_{<\omega}(\text{Seq}(9 \cup \text{Vbl} \cup \text{Const}_{\cup \text{ran}(f)})), \\ \text{Seq}(\mathcal{P}_{<\omega}(\text{Seq}(9 \cup \text{Vbl} \cup \text{Const}_{\cup \text{ran}(f)}))), \\ \text{Seq}(\text{Seq}(9 \cup \text{Vbl} \cup \text{Const}_{\cup \text{ran}(f)})), \\ \text{Seq}(9 \cup \text{Vbl} \cup \text{Const}_{\cup \text{ran}(f)}), \quad \text{Seq}(\mathcal{P}_{<\omega}(\text{Vbl})), \end{aligned}$$

where $\text{Seq}(x)$ = the set of all finite sequences from x , $\mathcal{P}_{<\omega}(x)$ = the set of all finite subsets of x . Hence, if we define the function w by

$$\begin{aligned} w(f) = \omega \cup \mathcal{P}_{<\omega}(\text{Seq}(9 \cup \text{Vbl} \cup \text{Const}_{\cup \text{ran}(f)})) \\ \cup \text{Seq}(\mathcal{P}_{<\omega}(\text{Seq}(9 \cup \text{Vbl} \cup \text{Const}_{\cup \text{ran}(f)}))) \\ \cup \text{Seq}(\text{Seq}(9 \cup \text{Vbl} \cup \text{Const}_{\cup \text{ran}(f)})) \\ \cup \text{Seq}(9 \cup \text{Vbl} \cup \text{Const}_{\cup \text{ran}(f)}) \cup \text{Seq}(\mathcal{P}_{<\omega}(\text{Vbl})), \end{aligned}$$

we obtain a definition of the form

$$y = L_\alpha \leftrightarrow \exists f \exists w [w = w(f) \wedge U(w, f, \alpha)],$$

where $U(w, f, \alpha)$ is the Σ_0 predicate obtained from the original definition of the function by deleting the initial existential quantifier and binding all remaining quantifiers which are not already bound, by w . To show that this is Σ_1 , we must show that the function $w(f)$ is Σ_1 . This reduces to showing that the functions $\text{Seq}(x)$ and $\mathcal{P}_{<\omega}(x)$ are Σ_1 . And since $y = \mathcal{P}_{<\omega}(x) \leftrightarrow \exists z [z = \text{Seq}(x) \wedge y = \{\text{ran}(u) \mid u \in z\}]$, this in turn reduces to showing that the function $\text{Seq}(x)$ is Σ_1 . Well,

$$y = \text{Seq}(x) \leftrightarrow$$

$$\leftrightarrow \exists g [g \text{ is a sequence} \wedge \text{dom}(g) = \omega \wedge y = \bigcup \text{ran}(g) \wedge g(0) = \emptyset \wedge$$

$$\forall n \in \omega \forall s \in g(n+1) \exists t \in g(n) \exists a \in x (s = t \cup \{\langle a, n \rangle\}) \wedge$$

$$\forall n \in \omega \forall s \in g(n) \forall a \in x \exists t \in g(n+1) (t = s \cup \{\langle a, n \rangle\}).$$

This is clearly Σ_1 . Moreover, this definition works for any limit L_λ above ω ; for if $x \in L_\alpha$, then $\text{Seq}(x) \subseteq L_{\alpha+2}$, so by the definition of $L_{\alpha+3}$ from $L_{\alpha+2}$, $\text{Seq}(x) \in L_{\alpha+3}$, and the unique g satisfying the above condition lies in $L_{\alpha+4}$.

It remains only to show that our final definition of the hierarchy function is suitable for any limit L_λ above ω . Well, there is clearly only one possibility for the function f , namely $\langle L_\nu \mid \nu \leq \alpha \rangle$. And by an easy induction on α we can show that $\alpha < \lambda$ implies $\langle L_\nu \mid \nu \leq \alpha \rangle \in L_\lambda$. The lemma is proved. $\square$

4.2. COROLLARY. *The function $\langle L_\nu \mid \nu \in \text{On} \rangle$ is Δ_1^{ZF} and uniformly Δ_1^{L} for limit $\lambda > \omega$.*

PROOF. In general, any Σ_1 function with a Π_1 domain is Δ_1 . To see this, consider the equivalence: $y = f(x) \leftrightarrow x \in \text{dom}(f) \wedge \forall z [z = f(x) \rightarrow x = y]$. $\square$

5. The axiom of constructibility

This is the assertion that *all* sets are constructible, and is usually written as $V = L$. By 4.2, we have at once:

5.1. LEMMA. (i) *The class L is Σ_1^{ZF} .*

(ii) *$V = L$ is a Π_2 formula of $\mathcal{L}$.*

PROOF. $x \in L \leftrightarrow \exists \alpha [x \in L_\alpha]$, so L is Σ_1 . And $V = L \leftrightarrow \forall x \exists \alpha (x \in L_\alpha)$. $\square$

4.2 also gives us (by the absoluteness of Δ_1 properties):

- 5.2. LEMMA.** (i) *If M is a transitive model of ZF, then for all $\alpha \in M$, $L_\alpha \in M$ and $(L_\alpha)^M = L_\alpha$. Hence $(L)^M = L_\lambda$ if $\lambda = \text{On} \cap M$ and $(L)^M = L$ if $\text{On} \subseteq M$.*
 (ii) *For all α , $(L_\alpha)^L = L_\alpha$. Hence $(L)^L = L$.*
 (iii) *If $\lim(\lambda)$ and $\lambda > \omega$, then $(L)^{L_\lambda} = L_\lambda$.*

By part (ii) of the above, we have at once:

5.3. THEOREM (Gödel). $\text{ZF} \vdash (V = L)^L$.

It should be pointed out that the use of the word “axiom” here is not intended to convey the idea that $V = L$ is a “reasonable” or “intuitive” addition to the axioms of ZFC as a basis for set theory. It is just that $V = L$ is an interesting additional assumption, worthy of study both in its own right and because it resolves many of the questions known to be undecidable on the basis of ZFC alone. (See our introductory remarks.) Moreover, any result proved in the system $\text{ZFC} + V = L$ will automatically be shown to be relatively consistent to ZF. (Because the construction of the constructible universe took place in ZF.)

6. The axiom of choice in L

We show that the axiom of choice is valid in L in a very strong way, by giving a formula which defines, over L, a well-ordering of L. The idea behind our definition is to fix a specific “order of construction” for the elements of L. In order to do this, it is convenient to “normalise” the definition of the constructible hierarchy slightly.

6.1. LEMMA. *For each α , there is an L_α -definable function $\langle -, - \rangle^\alpha$ on L_α such that:*

- (i) L_α is closed under $\langle -, - \rangle^\alpha$.
 (ii) *For all $x, y, x', y' \in L_\alpha$, $\langle x, y \rangle^\alpha = \langle x', y' \rangle^\alpha \leftrightarrow x = x' \wedge y = y'$.*

PROOF. If $\lim(\alpha)$, then the usual pairing function $\langle -, - \rangle$ suffices, of course. For all other cases, we define $\langle -, - \rangle^\alpha$ by recursion on α . Suppose $\langle -, - \rangle^\alpha$ has been defined. Thus $\langle -, - \rangle^\alpha \in L_{\alpha+1}$. So for $x, y \in L_{\alpha+1}$, we can define, in

$L_{\alpha+1}, x \times^{\alpha+1} y = \{\langle u, v \rangle^\alpha \mid u \in x \wedge v \in y\}$. We can then define, in $L_{\alpha+1}$, $\langle x, y \rangle^{\alpha+1} = (x \times^{\alpha+1} \{0\}) \cup (y \times^{\alpha+1} \{1\})$. $\square$

We call $\langle -, - \rangle^\alpha$ the α -pairing function. Using it, we have:

6.2. LEMMA. *If $x \in L_{\alpha+1}$, then for some $\mathcal{L}$ -formula $\varphi(v_0, v_1)$ and some $p \in L_\alpha$, $x = \{z \in L_\alpha \mid \models_{L_\alpha} \varphi(\dot{z}, \dot{p})\}$.*

PROOF. By “contraction of parameters” using the α -pairing function (and its L_α -definable inverses). $\square$

6.3. LEMMA. *There is a sequence $\langle <_\alpha \mid \alpha \in \text{On} \rangle$ such that:*

- (i) $\langle <_\alpha \mid \alpha \in \text{On} \rangle$ is Δ_1^{ZF} and uniformly Δ_1^{L} for limit $\lambda > \omega$;
- (ii) for limit $\lambda > \omega$, $<_\lambda$ is a (uniformly) Δ_1^{L} well-ordering of L_λ ;
- (iii) if $\alpha < \beta$, then $<_\beta$ is an end-extension of $<_\alpha$;
- (iv) if $x \in y \in L_\alpha$, then $x <_\alpha y$;
- (v) for limit $\lambda > \omega$, the function $\text{pr}(x) = \{y \mid y <_\lambda x\}$ is (uniformly) Δ_1^{L} .

PROOF. We define $<_\alpha$ by recursion on α . Set $<_0 = \emptyset$. And if $\lim(\lambda)$, $\lambda > 0$, set $<_\lambda = \bigcup_{\alpha < \lambda} <_\alpha$. Suppose now that $<_\alpha$ has been defined. Let $\langle \varphi_n \mid n < \omega \rangle$ be some recursive enumeration of the formulas of $\mathcal{L}$ with the free variables v_0 and v_1 . (We regard this enumeration as fixed from now on.) For $x \in L_{\alpha+1}$, set:

$n(x) =$ the least n such that for some $p \in L_\alpha$, $x = \{z \in L_\alpha \mid \models_{L_\alpha} \varphi_n(\dot{z}, \dot{p})\}$,

$p(x) =$ the $<_\alpha$ -least such p .

Then, for $x, y \in L_{\alpha+1}$, we set:

$$\begin{aligned} x <_{\alpha+1} y &\leftrightarrow [x, y \in L_\alpha \wedge x <_\alpha y] \vee \\ &\quad [x \in L_\alpha \wedge y \notin L_\alpha] \vee \\ &\quad [x, y \notin L_\alpha \wedge n(x) < n(y)] \vee \\ &\quad [x, y \notin L_\alpha \wedge n(x) = n(y) \wedge p(x) <_\alpha p(y)]. \end{aligned}$$

Clearly, each $<_\alpha$ is a well-ordering of L_α . Since $<_{\alpha+1}$ is always an end-extension of $<_\alpha$, condition (iii) is immediate. Condition (iv) is also immediate. The proof of (i) is very similar to the proof of 4.1 (and 4.2), so we omit the tedious details. For (ii), we have the Σ_1 definition $x <_\lambda y \leftrightarrow \exists \alpha < \lambda (x <_\alpha y)$, and hence also the Π_1 definition $x <_\lambda y \leftrightarrow x \neq y \wedge \neg \exists \alpha < \lambda (y <_\alpha x)$. And for (v), we have the Σ_1 definition

$$z = \text{pr}(x) \leftrightarrow \exists \nu < \lambda [x \in L_\nu \wedge z = \{y \mid y <_\nu x\}],$$

so as in 4.2, this function is Δ_1 . $\square$

We set $<_L = \bigcup_{\alpha \in \text{On}} <_\alpha$. Thus $<_L$ is a Σ_1^{ZF} well-ordering of L such that $<_L \cap (L_\lambda \times L_\lambda) = <_\lambda$ for all limit λ . Letting φ be the obvious Σ_1 $\mathcal{L}$ -formula which defines $<_L$, and ψ the Π_1 -formula $v_0 \neq v_1 \wedge \neg \varphi(v_1, v_0)$, we thus have:

6.4. THEOREM (Gödel; Jensen–Karp). *There are $\mathcal{L}$ -formulas φ and ψ , Σ_1 and Π_1 , respectively, such that:*

- (i) φ and ψ are absolute for L ;
- (ii) $\text{ZF} \vdash “\{\langle x, y \rangle \mid \varphi(x, y)\} \text{ well-orders } L”$;
- (iii) $\text{ZF} + V = L \vdash [\varphi(x, y) \leftrightarrow \psi(x, y)]$.

Hence, in particular, $\text{ZF} \vdash (\text{AC})^L$.

7. The condensation lemma. The GCH in L

We write $X <_{\Sigma_n} L_\alpha$ iff $X \subseteq L_\alpha$ and for every Σ_n sentence φ of $\mathcal{L}_X$, $\models_x \varphi$ iff $\models_{L_\alpha} \varphi$.

Clearly, if $X \subseteq L_\alpha$ is transitive, then $X <_{\Sigma_0} L_\alpha$. And for $\lim(\alpha)$, $n > 0$, $X <_{\Sigma_n} L_\alpha$ iff for all $P \in \mathcal{P}(L_\alpha) \cap \Sigma_n^{\text{tc}}(X)$, $P \neq \emptyset \rightarrow P \cap X \neq \emptyset$.

7.1. LEMMA (Condensation Lemma). *Suppose $\lim(\alpha)$. Let $X <_{\Sigma_1} L_\alpha$. Then there are unique β, π such that:*

- (i) $\pi : \langle X, \in \rangle \cong \langle L_\beta, \in \rangle$;
- (ii) if $Y \subseteq X$ is transitive, then $\pi \upharpoonright Y = \text{id} \upharpoonright Y$;
- (iii) $\pi(x) \leq_L x$ for all $x \in X$.

PROOF. If $\alpha = \omega$, then we must have $X = L_\omega$, so there is nothing further to prove. So we may assume that $\alpha > \omega$. Since $X <_{\Sigma_1} L_\alpha$ and L_α is transitive, X is well-founded and extensional. Hence by the well-known Mostowski Collapsing Lemma, there is a unique transitive set M and a unique isomorphism $\pi : X \cong M$. (This is discussed in 3.7 of Chapter A.7.) We show that $M = L_\beta$ for some (unique) β .

By 4.2, there is a Σ_0 formula $\varphi(v_0, v_1, v_2)$ such that:

- (a) $v = L_\gamma \leftrightarrow \models \exists z \varphi(z, v, \gamma)$;
- (b) $\models_{L_\alpha} \forall \gamma \exists v \exists z \varphi(z, v, \gamma)$;
- (c) $\models_{L_\alpha} \forall x \exists \gamma \exists v \exists z [\varphi(z, v, \gamma) \wedge x \in v]$.

Since $\pi^{-1} : M <_{\Sigma_1} L_\alpha$, (b) and (c) give:

- (d) $\forall \gamma \in M [\models_M \exists v \exists z \varphi(z, v, \gamma)]$;
- (e) $\forall x \in M [\models_M \exists \gamma \exists v \exists z [\varphi(z, v, \gamma) \wedge x \in v]]$.

Since Σ_0 statements are absolute for transitive sets, (d) and (e) give:

(f) $\forall \gamma \in M \exists v \in M \exists z \in M [\models \varphi(z, v, \gamma)]$;

(g) $\forall x \in M \exists \gamma \in M \exists v \in M \exists z \in M [\models \varphi(z, v, \gamma) \wedge x \in v]$.

Using (a), (f) and (g) give:

(h) $\forall \gamma \in M (L_\gamma \in M)$;

(i) $\forall x \in M \exists \gamma \in M (x \in L_\gamma)$.

Since M is transitive, (h) gives $\bigcup_{\gamma \in M} L_\gamma \subseteq M$. And by (i), $M \subseteq \bigcup_{\gamma \in M} L_\gamma$. Hence $M = \bigcup_{\gamma \in M} L_\gamma$. But as M is transitive, $M \cap \text{On} = \beta$, some ordinal β . And as $\pi^{-1} : M <_{\Sigma_1} L_\alpha$ and $\text{lim}(\alpha)$, we clearly have $\text{lim}(\beta)$. Hence $M = L_\beta$.

Part (i) of the lemma is thus proved. And part (ii) holds by the definition of the map π . For part (iii), suppose that $\pi(x) >_L x$ for some $x \in X$. Let x_0 be the least such x . Since $\pi : X \cong L_\beta$ and L_β is "closed" under $<_L$ and $x_0 <_L \pi(x_0)$, $x_0 \in L_\beta$. Hence for some $x_1 \in X$, $x_0 = \pi(x_1)$. Thus $\pi(x_1) <_L \pi(x_0)$. So, as $<_L$ is uniformly Σ_1^* for limit $\lambda > \omega$, $x_1 <_L x_0$. Thus by choice of x_0 , $\pi(x_1) = x_1$, contrary to $\pi(x_1) = x_0$. $\square$

Using 7.1, we can prove that the GCH holds in L . First a lemma.

7.2. LEMMA. *Let κ be a cardinal in L . If $x \in L$ is a bounded subset of κ , or if $x \subseteq L_\alpha$ for some $\alpha < \kappa$, then $x \in L_\kappa$.*

PROOF. Pick $\alpha < \kappa$ with $x \subseteq L_\alpha$. Pick λ such that $\text{lim}(\lambda)$ and $x \in L_\lambda$. Let M be the set of all elements of L_λ which are L_λ -definable from elements of $L_\alpha \cup \{x\}$. Since $<_L$ is L_λ -definable, it is easily seen that $M < L_\lambda$. So by 7.1, let $\pi : M \cong L_\gamma$. Notice that $\pi \upharpoonright L_\alpha = \text{id} \upharpoonright L_\alpha$, so in particular $\pi(x) = x$. (Recall that $\pi(x) = \{\pi(z) \mid z \in x \cap M\}$.) Hence $x \in L_\gamma$. Now, as our language is countable, $|M|^L = |L_\alpha|^L + \omega$. And by an easy induction argument, $|L_\nu|^L = |\nu|^L$ for all infinite ν . Hence $|\gamma|^L \leq |\alpha|^L + \omega < \kappa$. Hence $\gamma < \kappa$, and $x \in L_\kappa$. $\square$

7.3. THEOREM (Gödel). $\text{ZF} \vdash (\text{GCH})^L$.

PROOF. By 7.2, for all infinite κ , $2^\kappa \leq |L_{\kappa^+}|$. But $|L_{\kappa^+}| = \kappa^+$. Hence $2^\kappa = \kappa^+$. $\square$

8. Σ_1 Skolem functions

An important concept in constructibility theory is that of a Σ_1 Skolem function.

A Σ_1 Skolem function for L_α is a Σ_1^L function h such that $\text{dom}(h) \subseteq$

$\omega \times L_\alpha$, $\text{ran}(h) \subseteq L_\alpha$, and whenever $P \in \Sigma_1^{\text{L}_\alpha}(\{x\}) \cap \mathcal{P}(L_\alpha)$ for some $x \in L_\alpha$, then $\exists y P(y) \rightarrow \exists i \in \omega P(h(i, x))$.

8.1. LEMMA. *Let $\lim(\alpha)$, and let h be a Σ_1 Skolem function for L_α . If $x \in L_\alpha$, then $x \in h''(\omega \times \{x\}) <_{\Sigma_1} L_\alpha$.*

PROOF. Set $N = h''(\omega \times \{x\})$. Clearly, $x \in N$. Let $P \in \Sigma_1^{\text{L}_\alpha}(N) \cap \mathcal{P}(L_\alpha)$. We show that $P \neq \emptyset \rightarrow P \cap N \neq \emptyset$. Pick $y_1, \dots, y_m \in N$ with $P \in \Sigma_1^{\text{L}_\alpha}(\{y_1, \dots, y_m\})$. By definition of N there are $j_1, \dots, j_m \in \omega$ with $y_1 = h(j_1, x), \dots, y_m = h(j_m, x)$. Since h is $\Sigma_1^{\text{L}_\alpha}$, it follows that $P \in \Sigma_1^{\text{L}_\alpha}(\{x\})$. Hence $P \neq \emptyset \rightarrow \exists y P(y) \rightarrow \exists i \in \omega P(h(i, x)) \rightarrow \exists y \in NP(y) \rightarrow P \cap N \neq \emptyset$. $\square$

8.1 may be generalised in several ways. For instance:

8.2. LEMMA. *Let $\lim(\alpha)$, and let h be a Σ_1 Skolem function for L_α . If $p \in L_\alpha$ and if $X \subseteq L_\alpha$ is closed under ordered pairs, then $X \cup \{p\} \subseteq h''(\omega \times (X \times \{p\})) <_{\Sigma_1} L_\alpha$.*

PROOF. Set $N = h''(\omega \times (X \times \{p\}))$. Clearly, $X \cup \{p\} \subseteq N$. Let $P \in \Sigma_1^{\text{L}_\alpha}(N) \cap \mathcal{P}(L_\alpha)$, $P \neq \emptyset$. Pick $y_1, \dots, y_m \in N$ with $P \in \Sigma_1^{\text{L}_\alpha}(\{y_1, \dots, y_m\})$. Pick $j_1, \dots, j_m \in \omega$ and $x_1, \dots, x_m \in X$ with $y_1 = h(j_1, \langle x_1, p \rangle), \dots, y_m = h(j_m, \langle x_m, p \rangle)$. Let $x = \langle x_1, \dots, x_m \rangle$. By assumption on X , $x \in X$. And as h is $\Sigma_1^{\text{L}_\alpha}$, P is $\Sigma_1^{\text{L}_\alpha}(\{\langle x, p \rangle\})$. So, $P \neq \emptyset \rightarrow \exists y P(y) \rightarrow \exists i \in \omega P(h(i, \langle x, p \rangle)) \rightarrow \exists y \in NP(y) \rightarrow P \cap N \neq \emptyset$, and the lemma is proved. $\square$

Similarly, we have:

8.3. LEMMA. *Let $\lim(\alpha)$, and let h be a Σ_1 Skolem function for L_α . If $X \subseteq L_\alpha$ and if $h''(\omega \times X)$ is closed under ordered pairs, then $X \subseteq h''(\omega \times X) <_{\Sigma_1} L_\alpha$.*

PROOF. Clearly, if $Y = h''(\omega \times X)$, then $h''(\omega \times Y) = h''(\omega \times X)$, so the result follows from 8.2. $\square$

The above two lemmas give the forms in which Σ_1 Skolem functions are often used. As to the existence of Σ_1 Skolem functions, we show below that for each limit ordinal $\alpha > \omega$, L_α has a Σ_1 Skolem function. We require some preliminaries.

8.4. LEMMA. *Let $\lim(\alpha)$, $\alpha > \omega$. Then $\models_{L_\alpha}^{\Sigma_0}$ (the restriction of $\models_{L_\alpha}$ to the Σ_0 sentences of $\mathcal{L}_{L_\alpha}$) is (uniformly) $\Sigma_1^{\text{L}_\alpha}$.*

PROOF. For any Σ_0 sentence φ of $\mathcal{L}_{L_\alpha}$, we have, by absoluteness, $\models_{L_\alpha} \varphi$ iff $\models_{\text{TC}(\text{ran}(\varphi))} \varphi$, where $\text{TC}(x)$ denotes the transitive closure of x . Hence, with $\text{Sat}(u, \varphi)$ the predicate defined in Section 3, we have, for Σ_0 φ , $\models_{L_\alpha} \varphi$ iff $\text{Sat}(\text{TC}(\text{ran}(\varphi)), \varphi)$. Now, by examining the definition of Sat , we see easily that in the relation $\text{Sat}(u, \varphi)$, any unbounded quantifiers may be bound by a set of the form $w = w(u)$, where w is a Σ_1 function similar to the one used in 4.1. Hence $\text{Sat}(u, \phi)$ has the Σ_1^L definition

$$\text{Sat}(u, \phi) \leftrightarrow \exists w [w = w(u) \wedge S(w, u, \phi)],$$

where $S(w, u, \varphi)$ is the Σ_0 formula obtained from the definition of Sat given in Section 3, by binding all unbounded quantifiers by w . But the function TC is also Σ_1^L , having the definition

$$w = \text{TC}(x) \leftrightarrow \exists f [f \text{ is a function} \wedge \text{dom}(f) = \omega \wedge f(0) = x \wedge \forall n \in \omega (f(n+1) = \bigcup f(n)) \wedge w = \bigcup \text{ran}(f)].$$

Hence $\models_{L_\alpha}^{\Sigma_0}$ is Σ_1^L . $\square$

8.5. COROLLARY. *Let $\lim(\alpha)$, $\alpha > \omega$. Then $\models_{L_\alpha}^{\Sigma_1}$ (the restriction of $\models_{L_\alpha}$ to the sentences of $\mathcal{L}_{L_\alpha}$ of the form $\exists v_0 \varphi(v_0)$, where φ is Σ_0) is (uniformly) Σ_1^L .*

PROOF. Let Sub be the function as defined in Section 3. Arguing much as we did for Sat in 8.4, we see that $\text{Sub}(\varphi, v, t)$ is Σ_1^L . But if $\bar{\varphi}$ is Σ_0 and $\varphi = \exists v_0 \bar{\varphi}$, then

$$\models_{L_\alpha} \varphi \quad \text{iff} \quad \exists \psi \in L_\alpha \exists x \in L_\alpha [\varphi = \exists v_0 \psi \ \& \ \models_{L_\alpha}^{\Sigma_0} \text{sup}(\psi, v_0, \dot{x})],$$

so we are done. $\square$

8.6. LEMMA. *Let $\lim(\alpha)$, $\alpha > \omega$. Then L_α has a (uniformly Σ_1^L) Σ_1 Skolem function.*

PROOF. Let $\langle \varphi_i \mid i < \omega \rangle$ be a (fixed, canonical) recursive enumeration of all formulas of $\mathcal{L}$ of the form $\varphi_i = \exists v_0 \bar{\varphi}_i(v_0, v_1, v_2)$, where $\bar{\varphi}_i$ is Σ_0 . Define a (partial) function r_α by:

$$\begin{aligned} w = r_\alpha(i, x) &\leftrightarrow \models_{L_\alpha} \bar{\varphi}_i((\dot{w})_0, (\dot{w})_1, \dot{x}) \wedge \forall z <_L \dot{w} \neg \bar{\varphi}_i((z)_0, (z)_1, \dot{x}) \\ &\leftrightarrow \models_{L_\alpha} \bar{\varphi}_i((\dot{w})_0, (\dot{w})_1, \dot{x}) \wedge \exists u [u = \{z \mid z <_L \dot{w}\} \wedge \\ &\quad \forall z \in u \neg \bar{\varphi}_i((z)_0, (z)_1, \dot{x})]. \end{aligned}$$

By 8.5 (together with 6.3), r_α is Σ_1^L . Hence h_α is Σ_1^L , where we set: $h_\alpha(i, x) = (r_\alpha(i, \dot{x}))_1$. It is easily seen that h_α is as required. $\square$

We call the function h_α defined above the *canonical* Σ_1 Skolem function for L_α . Let H_i be the Σ_0 formula of $\mathcal{L}$, implicitly given by the above proof, such that for all limit $\alpha > \omega$, and all $x, y \in L_\alpha$, $y = h_\alpha(i, x) \leftrightarrow \exists z \in L_\alpha [\models_{L_\alpha} H_i(\hat{z}, \hat{y}, \hat{x})]$. In particular, notice that the sequence $\langle H_i \mid i < \omega \rangle$ will be recursive, so (by 8.5) H_α will be (uniformly) $\Sigma_1^{\perp\alpha}$ (for limit $\alpha > \omega$), where $H_\alpha(z, y, i, x) \leftrightarrow \models_{L_\alpha} H_i(\hat{z}, \hat{y}, \hat{x})$. We fix this notation from now on.

As an example of the use of Σ_1 Skolem functions, we prove:

8.7. LEMMA. *Let $\lim(\alpha)$, $\alpha > \omega$. Then there is a $\Sigma_1(L_\alpha)$ map of α onto L_α .*

PROOF. By means of a technical, though not unduly difficult argument, we may show that there is a $\Sigma_1(L_\alpha)$ map of α onto $\alpha \times \alpha$. So, let $p \in L_\alpha$ be such that there is a $\Sigma_1^{\perp\alpha}(\{p\})$ map of α onto $\alpha \times \alpha$, p the $<_L$ -least such, and let f be a $\Sigma_1^{\perp\alpha}(\{p\})$ map of α onto $\alpha \times \alpha$. Define f^0, f^1 by $f(\nu) = \langle f^0(\nu), f^1(\nu) \rangle$, all $\nu \in \alpha$. By recursion, define $f_n : \alpha \xrightarrow{\text{onto}} \alpha^n$ by: $f_i = \text{id} \upharpoonright \alpha$; $f_{n+1}(\nu) = \langle f^0(\nu), f_n \circ f^1(\nu) \rangle$. Thus each f_n in $\Sigma_1^{\perp\alpha}(\{p\})$. Let $h = h_\alpha$, and set $X = h''(\omega \times (\alpha \times \{p\}))$.

Claim 1. X is closed under ordered pairs.

To see this, let $x_1, x_2 \in X$. Pick $j_1, j_2 \in \omega$ and $\nu_1, \nu_2 \in \alpha$ with $x_1 = h(j_1, \langle \nu_1, p \rangle)$, $x_2 = h(j_2, \langle \nu_2, p \rangle)$. Let $\langle \nu_1, \nu_2 \rangle = f_2(\tau)$. Then $\{\langle x_1, x_2 \rangle\}$ is a $\Sigma_1^{\perp\alpha}(\{\langle \tau, p \rangle\})$ predicate. So, by definition of h , $\langle x_1, x_2 \rangle \in X$, which proves the claim.

By the claim and 8.3, $X <_{\Sigma_1} L_\alpha$. By the condensation lemma, let $\pi : X \cong L_\beta$. Since $\alpha \subseteq X$, we clearly have $\beta = \alpha$ here.

Claim 2. For all $i \in \omega$ and all $x \in X$, $\pi(h(i, x)) = h(i, \pi(x))$.

To see this, suppose first that $i \in \omega$, $x \in X$, and $y = h(i, x)$. Since h is $\Sigma_1^{\perp\alpha}$ and $x \in X <_{\Sigma_1} L_\alpha$, $y \in X$. And as $y = h(i, x)$, $\models_{L_\alpha} \exists z H_i(z, \hat{y}, \hat{x})$, so $\models_X \exists z H_i(z, \hat{y}, \hat{x})$, so for some $z \in X$, $\models_X H_i(\hat{z}, \hat{y}, \hat{x})$. Applying π , $\models_{L_\alpha} H_i(\pi(z)^\circ, \pi(y)^\circ, \pi(x)^\circ)$. Hence $\models_{L_\alpha} \exists z H_i(z, \pi(y)^\circ, \pi(x)^\circ)$. Thus $\pi(y) = h(i, \pi(x))$. Conversely, if $h(i, \pi(x))$ is defined, then we must have $h(i, \pi(x)) = \pi(y)$ for some y , and we can reverse the above steps to obtain $y = h(i, x)$. This proves the claim.

Now, $f \subseteq \alpha \times \alpha \times \alpha$ and $\pi \upharpoonright \alpha = \text{id} \upharpoonright \alpha$, so $\pi''f = f$. And by isomorphism, $\pi''f$ is $\Sigma_1^{\perp\alpha}(\{\pi(p)\})$. So by choice of p , $p \leq_L \pi(p)$. But by the condensation lemma, $\pi(p) \leq_L p$. Hence $\pi(p) = p$. So by claim 2, if $i \in \omega$ and $\nu < \alpha$, $\pi(h(i, \langle \nu, p \rangle)) = h(i, \langle \nu, p \rangle)$. Hence $\pi \upharpoonright X = \text{id} \upharpoonright X$. Hence $X = L_\alpha$.

Let S be a $\Sigma_0^{\perp\alpha}$ predicate such that

$$y = h(i, x) \leftrightarrow \exists z \in L_\alpha S(z, y, i, x).$$

Define $g : \alpha \times \alpha \times \alpha \rightarrow L_\alpha$ by

$$g(i, \nu, \tau) = \begin{cases} y & \text{if } y \in L_\tau \text{ \& } \exists z \in L_\tau S(z, y, i, \langle \nu, p \rangle), \\ \emptyset & \text{otherwise.} \end{cases}$$

Then g has the $\Sigma_1(L_\alpha)$ definition

$$y = g(i, \nu, \tau) \leftrightarrow [y \in L_\tau \text{ \& } \exists z \in L_\tau S(z, y, i, \langle \nu, p \rangle)] \vee \\ [\forall y' \in L_\tau \forall z \in L_\tau \neg S(z, y', i, \langle \nu, p \rangle) \wedge y = \emptyset].$$

And clearly, $g''(\alpha \times \alpha \times \alpha) = h''(\omega \times (\alpha \times \{p\})) = X = L_\alpha$. Hence $g \circ f_3$ is as required. $\square$

9. Admissible ordinals

An *admissible set* is, it will be recalled, a transitive set M which satisfies the following conditions:

- (I) $M \neq \emptyset$,
- (II) $\forall x \in M (\bigcup x \in M)$,
- (III) $\forall x, y \in M (\{x, y\} \in M)$,
- (IV) $\forall u \in M (P \cap u \in M)$, where $P \in \Sigma_0(M) \cap \mathcal{P}(M)$ (Σ_0 -Comprehension),
- (V) $\forall x \in M \exists y \in M P(y, x) \rightarrow \forall u \in M \exists v \in M \forall x \in u \exists y \in v P(y, x)$, where $P \in \Sigma_0(M) \in \mathcal{P}(M)$ (Σ_0 -Replacement, or, more accurately, Σ_0 -Collection).

Moreover, if M is an admissible set, we may show that in fact (IV) and (V) hold for the case where P is $\Delta_1(M)$ and $\Sigma_1(M)$, respectively, thereby obtaining the principles of Δ_1 -Comprehension and Σ_1 -Replacement. See Section 2 of Chapter A.7 on admissible sets.

An ordinal α is *admissible* just in case L_α is an admissible set. (It is not hard to show that α will be admissible iff there is an admissible set M with $\alpha = M \cap \text{On}$, so the dependence of our definition upon the constructible hierarchy here is only apparent.)

It is easily seen that if $\lim(\alpha)$, then L_α satisfies (I)–(IV) of the definition of admissibility. Hence:

9.1. LEMMA. *Let $\lim(\alpha)$. Then α is admissible iff for each $\Sigma_0(L_\alpha)$ predicate $P(y, x)$ on L_α ,*

$$\forall x \in L_\alpha \exists y \in L_\alpha P(y, x) \rightarrow \forall u \in L_\alpha \exists v \in L_\alpha \forall x \in u \exists y \in v P(y, x).$$

Using 9.1, we have:

9.2. LEMMA. *Let $\lim(\alpha)$. Then α is admissible iff there is no $\Sigma_1(L_\alpha)$ mapping from an ordinal $\delta < \alpha$ cofinally into α .*

REMARK. Suppose α is admissible. Let $f: \delta \rightarrow \alpha$ be $\Sigma_1(L_\alpha)$, where $\delta < \alpha$. Then $\forall \xi \in \delta \exists \zeta (\zeta = f(\xi))$. So by Σ_1 -Replacement there is $\gamma \in \alpha$ with $\forall \xi \in \delta \exists \zeta \in \gamma (\zeta = f(\xi))$. Hence $f''\delta \subseteq \gamma$, and f is not cofinal.

Conversely, suppose there is no $\Sigma_1(L_\alpha)$ mapping from an ordinal $\delta < \alpha$ cofinally into α . Using 9.1, we show that L_α is admissible. Let $P(y, x)$ be a $\Sigma_0(L_\alpha)$ predicate such that $\forall x \in L_\alpha \exists y \in L_\alpha P(y, x)$. Let $u \in L_\alpha$ be given. We seek a $v \in L_\alpha$ such that $\forall x \in u \exists y \in v P(y, x)$. Define a $\Sigma_1(L_\alpha)$ map $f: u \rightarrow \alpha$ by $f(x) =$ the least γ such that $\exists y \in L_\gamma P(y, x)$. Let δ be the least ordinal such that $u \subseteq L_\delta$. Extend f trivially to L_δ . By our assumption, together with 8.7, f cannot be cofinal in α . So there is a $\rho < \alpha$ with $f''L_\delta \subseteq \rho$. Hence $v = L_\rho$ is as sought. $\square$

Our next result strengthens 9.2 considerably.

9.3. LEMMA. *Let $\lim(\alpha)$. Then α is admissible iff there is no $\Sigma_1(L_\alpha)$ map from an ordinal $\delta < \alpha$ onto α .*

PROOF. ($\rightarrow$) This part follows directly from 9.2.

($\leftarrow$) Assume that α is not admissible. We show that there is a $\Sigma_1(L_\alpha)$ map from an ordinal $\delta < \alpha$ onto α . Now, by 9.2 we know that there is a $\delta < \alpha$ and a $\Sigma_1(L_\alpha)$ map f of δ cofinally into α . Let f be $\Sigma_1^{L_\alpha}(\{p\})$. If $\alpha = \gamma + \omega$ for some γ , we are clearly done. Hence we may assume otherwise, and pick a limit ordinal $\gamma < \alpha$ with $\delta, p \in L_\gamma$. Let $h = h_\alpha$. Set $X = h''(\omega \times L_\gamma)$. Since L_γ is closed under ordered pairs, $X <_{\Sigma_1} L_\alpha$. Let $\pi: X \cong L_\beta$. Since $\pi \upharpoonright L_\gamma = \text{id} \upharpoonright L_\gamma$, an argument as in the proof of claim 2 of 8.7 tells us that $\pi \upharpoonright X = \text{id} \upharpoonright X$. Hence $X = L_\beta$. Now, f is $\Sigma_1^{L_\alpha}(\{p\})$ and $p \in X <_{\Sigma_1} L_\alpha$, so X is closed under f . But $\delta \subseteq X$ and f is cofinal in α . Hence $\alpha \subseteq X$. Hence $\beta = \alpha$ and $X = L_\beta$.

Let S be a $\Sigma_0^{L_\alpha}$ predicate such that

$$y = h(i, x) \leftrightarrow \exists z \in L_\alpha S(z, y, i, x).$$

Define $g: \omega \times \delta \times L_\gamma \rightarrow L_\alpha$ by

$$g(i, v, x) = \begin{cases} y & \text{if } y \in L_{f(v)} \text{ \& } \exists z \in L_{f(v)} S(z, y, i, x), \\ \emptyset & \text{otherwise.} \end{cases}$$

As in the proof of 8.7, we see that g is $\Sigma_1^{L_\alpha}(\{p\})$. Moreover, $g''(\omega \times \delta \times L_\gamma) = h''(\omega \times L_\gamma) = X = L_\alpha$. But by 8.7 there is a $\Sigma_1(L_\gamma)$ map $j: \gamma \xrightarrow{\text{onto}} \omega \times \delta \times L_\gamma$. Hence $g \circ j$ is a $\Sigma_1(L_\alpha)$ map of γ onto L_α . $\square$

Chapter C.5 discusses recursion theory on admissible ordinals and its interaction with constructibility.

10. The Souslin hypothesis

Some of the best illustrations of the methods of constructibility theory are provided by the Souslin Hypothesis and its generalisations.

The *Souslin Hypothesis*, SH, is the assertion that whenever X is a dense linear ordering with no end-points, complete under the formation of sups and infs, and with the property that any collection of pairwise disjoint open intervals is countable, then X is isomorphic to the real line. (The real line clearly possesses all of the properties just stated.)

An old theorem of Miller characterises SH in terms of trees (see Theorem 4.11 of Chapter B.3). A *tree* is a poset $\mathbf{T} = \langle T, \leq \rangle$ such that $\hat{x} = \{y \in T \mid y < x\}$ is well-ordered by $<$ for all $x \in T$. The order-type of $\hat{x}$ under $<$ is called the *height* of x in $\mathbf{T}$, $\text{ht}(x)$. The α -th *level* of $\mathbf{T}$ is the set $T_\alpha = \{x \in T \mid \text{ht}(x) = \alpha\}$. We set $T \restriction \alpha = \bigcup_{\beta < \alpha} T_\beta$.

Let θ be a limit ordinal, λ a cardinal. $\mathbf{T}$ is a (θ, λ) -*tree* iff:

- (i) $\forall \alpha < \theta (0 < |T_\alpha| < \lambda) \wedge |T_0| = 1 \wedge T_\theta = \emptyset$,
- (ii) $\forall \alpha < \theta \forall x \in T_\alpha (|\{y \in T_{\alpha+1} \mid x < y\}| \geq 2)$,
- (iii) $\forall \alpha < \beta < \theta \forall x \in T_\alpha \exists y \in T_\beta (x < y)$,
- (iv) $\forall \alpha < \theta \forall x, y \in T_\alpha (\text{lim}(\alpha) \rightarrow (x = y \leftrightarrow \hat{x} = \hat{y}))$.

If κ is a cardinal, a κ -*tree* is a (κ, κ) -tree.

Let $\mathbf{T}$ be a tree. A *branch* of $\mathbf{T}$ is a maximal linearly ordered subset of $\mathbf{T}$. An antichain of $\mathbf{T}$ is a pairwise incomparable subset of $\mathbf{T}$. A branch of $\mathbf{T}$ is an α -*branch* if α is its order type. An *Aronszajn tree* is an ω_1 -tree with no ω_1 -branch. A classical theorem of Aronszajn is that such a tree exists (in ZFC). A *Souslin tree* is an ω_1 -tree with no uncountable antichain. It is easily seen that any Souslin tree is Aronszajn. The converse is not provable. Indeed, in ZFC it is not decidable whether or not a Souslin tree exists. (See DEVLIN and JOHNSBRÄTEN [1974] for details.) Miller's theorem is that SH is equivalent to the non-existence of a Souslin tree. The easy proof may be found in DEVLIN and JOHNSBRÄTEN [1974]. Hence SH is undecidable in ZFC. It is, however, decidable if we assume $V = L$.

10.1. THEOREM (Jensen). *Assume $V = L$. Then $\neg \text{SH}$.*

PROOF. We construct a Souslin tree $\mathbf{T}$ by recursion on the levels. The elements of $\mathbf{T}$ will be countable sequences of 0's and 1's, and the tree ordering will be ordinary inclusion. Moreover, $\mathbf{T}$ will be such that $s \subseteq t \in T \rightarrow s \in T$, whence $s \in T_\alpha \rightarrow s \in 2^\alpha$. To commence, we set $T_0 = \{\emptyset\}$. If T_α is defined, we set

$$T_{\alpha+1} = \{s \hat{\ } \langle 0 \rangle \mid s \in T_\alpha\} \cup \{s \hat{\ } \langle 1 \rangle \mid s \in T_\alpha\}.$$

Finally, suppose $\lim(\alpha)$ and that $T \restriction \alpha$ is defined. In order to define T_α we make use of the function $f: \omega_1 \rightarrow \omega_1$ defined by $f(\xi) =$ the least γ such that $\models_{L_\gamma}$ “ ξ is countable”. (To see that f is well-defined, use 7.2.) For each $x \in T \restriction \alpha$, let $s_x = \bigcup b_x$, where b_x is the $<_L$ -least α -branch of $T \restriction \alpha$ which contains x and which meets every maximal antichain of $T \restriction \alpha$ lying in $L_{f(\alpha)}$. Since $\text{cf}(\alpha) = \omega$ and $|L_{f(\alpha)}| = \omega$, b_x is always defined, whence so is s_x . And $s_x \in 2^\alpha$, of course. Let $T_\alpha = \{s_x \mid x \in T \restriction \alpha\}$. This defines $\mathbf{T} = \bigcup_{\alpha < \omega_1} T_\alpha$.

We show that $\mathbf{T}$ is a Souslin tree. Clearly, $\mathbf{T}$ is an ω_1 -tree. So, if $\mathbf{T}$ were not Souslin, we could find an uncountable maximal antichain of $\mathbf{T}$. Suppose then that A is the $<_L$ -least uncountable maximal antichain of $\mathbf{T}$. Now, by 7.2, $\mathbf{T} \in L_{\omega_2}$. And clearly, $\mathbf{T}$ is L_{ω_2} -definable. Hence $A \in L_{\omega_2}$ is also L_{ω_2} -definable. So, if M is the smallest $M < L_{\omega_2}$ (i.e. M is the set of all L_{ω_2} -definable elements of L_{ω_2}), $\mathbf{T}, A \in M$.

Claim: $M \cap \omega_1 \in \omega_1$.

Since M is clearly countable, to prove the claim, it suffices to show that $M \cap \omega_1$ is transitive. Let $\gamma \in M \cap \omega_1$. Since $\gamma \in \omega_1$, $\models_{L_{\omega_2}}$ “ γ is countable”. Let j be the $<_L$ -least map $j: \omega \xrightarrow{\text{onto}} \gamma$. Since $\gamma \in M < L_{\omega_2}$ and j is L_{ω_2} -definable from γ , $j \in M$. But $\omega \subseteq M$. Hence $\gamma = j''\omega \subseteq M$, and we are done.

By the claim, set $\alpha = M \cap \omega_1$. Let $\pi: M \cong L_\lambda$. Clearly, $\pi \restriction L_\alpha = \text{id} \restriction L_\alpha$, $\pi(\omega_1) = \alpha$, $\pi(\mathbf{T}) = \mathbf{T} \restriction \alpha$, $\pi(A) = A \cap \alpha = A \cap (T \restriction \alpha)$. Also, since $\models_{L_{\omega_2}}$ “ A is a maximal antichain of $\mathbf{T}$ ”, $\models_{L_\lambda}$ “ $A \cap \alpha$ is a maximal antichain of $T \restriction \alpha$ ”, so $A \cap \alpha$ really is a maximal antichain of $\mathbf{T} \restriction \alpha$. And of course $A \cap \alpha \in L_\lambda$. But look, $\alpha = \omega_1^{\text{L}}$ and α is countable in $L_{f(\alpha)}$, so we must have $\lambda < f(\alpha)$. Hence $A \cap \alpha \in L_{f(\alpha)}$. Hence, by definition of T_α , every element of T_α lies above an element of $A \cap \alpha$. Hence $A \cap \alpha$ is a maximal antichain in $\mathbf{T}$. Hence $A = A \cap \alpha$. But this is absurd, since A is uncountable. Hence $\mathbf{T}$ must be a Souslin tree, and we are done. $\square$

For a direct construction of a Souslin line see Theorem 3.8 of Chapter B.3.

11. The generalised Souslin hypothesis

The notion of a Souslin tree clearly generalises from ω_1 to any regular cardinal κ . Thus, a κ -Souslin tree is a κ -tree with no antichain of cardinality κ . (And any such tree will be a κ -Aronszajn tree, as in the case $\kappa = \omega_1$.) We denote by $\text{SH}(\kappa)$ the assertion that there is no κ -Souslin tree. By examining the proof of 10.1, we shall prove that if $V = L$, then $\text{SH}(\kappa)$

fails for all successor cardinals. Later on we shall consider the case of inaccessible cardinals.

Now, when one tries to generalise the proof of 10.1 to the case of an arbitrary successor cardinal, one runs into the problem that one must extend branches at limit levels of uncountable cofinality. And this is not always easy to do. For instance, in attempting to construct an ω_2 -Souslin tree T , already $T \upharpoonright \omega_1$ might be an Aronszajn tree, in which case one can go no further. In order to avoid such difficulties, one sets up (in L) some combinatorial machinery, and then uses this machinery to construct the Souslin tree. Unfortunately, due to the limitations of space, we cannot give any prior motivation for the machinery itself, but must rely upon its application to the construction of Souslin trees to provide such motivation.

Let κ be any cardinal, possibly singular. Let $E \subseteq \kappa^+$. By $\square_\kappa(E)$ we mean the following assertion: There is a sequence $\langle C_\lambda \mid \lambda < \kappa^+ \wedge \text{lim}(\lambda) \rangle$ such that:

- (i) C_λ is a closed unbounded subset of λ ;
 - (ii) $\text{cf}(\lambda) < \kappa \rightarrow |C_\lambda| < \kappa$;
 - (iii) if γ is a limit point of C_λ , then $\gamma \notin E$ and $C_\gamma = \gamma \cap C_\lambda$.
- (Notice that by (ii) and (iii) in the above, $\text{cf}(\lambda) = \kappa \rightarrow \text{otp}(C_\lambda) = \kappa$, where otp means order type.)

We denote $\square_\kappa(\emptyset)$ by $\square_\kappa$. In Section 13 we shall prove the following result:

11.1. THEOREM (Jensen). *Assume $V = L$. Let κ be any cardinal. Then there is a stationary set $E \subseteq \kappa^+$ such that $\alpha \in E \rightarrow \text{cf}(\alpha) = \omega$ and $\square_\kappa(E)$ holds. $\square$*

As well as $\square_\kappa$, we also require the following combinatorial principle. As for $\square_\kappa$, this principle is also due to Jensen.

Let κ be a regular cardinal, $E \subseteq \kappa$. By $\diamond_\kappa(E)$ we mean the assertion that there is a sequence $\langle S_\alpha \mid \alpha \in E \rangle$ such that $S_\alpha \subseteq \alpha$ and for every $X \subseteq \kappa$, the set $\{\alpha \in E \mid X \cap \alpha = S_\alpha\}$ is stationary in κ .

Of course, for $\diamond_\kappa(E)$ to hold, it is necessary that E itself be stationary in κ . Assuming $V = L$, this condition is also sufficient here.

11.2. THEOREM (Jensen). *Assume $V = L$. Let κ be any uncountable regular cardinal, and let E be any stationary subset of κ . Then $\diamond_\kappa(E)$ holds.*

PROOF. By recursion on $\alpha \in E$, define $\langle S_\alpha, C_\alpha \rangle$ as the $<_L$ -least pair such that $S_\alpha, C_\alpha \subseteq \alpha$, C_α is closed and unbounded in α , and $\gamma \in C_\alpha \cap E \rightarrow S_\alpha \cap \gamma \neq S_\gamma$; with $S_\alpha = C_\alpha = \emptyset$ if either $\text{succ}(\alpha)$ or else $\text{lim}(\alpha)$ but no such pair

exists. We claim that $\langle S_\alpha \mid \alpha \in E \rangle$ is as required. Well, suppose not. Let $\langle S, C \rangle$ be the $<_L$ -least pair such that $S, C \subseteq \kappa$, C is closed and unbounded in κ , and $\alpha \in C \cap E \rightarrow S \cap \alpha \neq S_\alpha$. Since $\langle S_\alpha \mid \alpha \in E \rangle$ is clearly definable from E in L_{κ^+} , so is $\langle S, C \rangle$. Define a sequence $\langle N_\nu \mid \nu < \kappa \rangle$ of elementary submodels of L_{κ^+} as follows:

N_0 = the smallest $N < L_{\kappa^+}$ such that $N \cap \kappa \in \text{On}$ and $E \in N$.

$N_{\nu+1}$ = the smallest $N < L_{\kappa^+}$ such that $N \cap \kappa \in \text{On}$ and $N_\nu \cup \{N_\nu\} \subseteq N$.

$N_\lambda = \bigcup_{\nu < \lambda} N_\nu$, if $\lim(\lambda)$.

Set $\alpha_\nu = N_\nu \cap \kappa$, each ν . Clearly, $\langle \alpha_\nu \mid \nu < \kappa \rangle$ is a strictly increasing, continuous sequence, cofinal in κ . So we can pick a ν such that $\alpha_\nu = \nu \in E \cap C$. Let $\pi : N_\nu \cong L_\beta$. Then $\pi \upharpoonright \nu = \text{id} \upharpoonright \nu$, $\pi(\kappa) = \nu$, and $\pi(\langle S, C \rangle) = \langle S \cap \nu, C \cap \nu \rangle$, and $\pi(\langle S_\alpha \mid \alpha \in E \rangle) = \langle S_\alpha \mid \alpha \in E \cap \nu \rangle$. And since $\pi^{-1} : L_\beta < L_{\kappa^+}$, $\langle S \cap \nu, C \cap \nu \rangle$ is the $<_L$ -least pair such that $S \cap \nu, C \cap \nu \subseteq \nu$, $C \cap \nu$ is closed and unbounded in ν , and $\gamma \in C \cap \nu \cap E \rightarrow S \cap \nu \cap \gamma \neq S_\gamma$. Hence $\langle S \cap \nu, C \cap \nu \rangle = \langle S_\nu, C_\nu \rangle$. In particular, $S \cap \nu = S_\nu$. But $\nu \in C \cap E$, so this contradicts the choice of $\langle S, C \rangle$. The proof is complete. $\square$

We are now in a position to show that $\text{SH}(\kappa)$ fails for all successor cardinals κ in L .

11.3. THEOREM (Jensen). *Let κ be any cardinal. Suppose that there is a stationary set $E \subseteq \kappa^+$ such that $\square_\kappa(E)$ and $\diamond_{\kappa^+}(E)$ hold. Then $\neg \text{SH}(\kappa^+)$.*

Hence (by 11.1 and 11.2) if $V = L$, then $\forall \kappa [\neg \text{SH}(\kappa^+)]$.

PROOF. Let $\langle C_\lambda \mid \lambda < \kappa^+ \wedge \lim(\lambda) \rangle$ satisfy $\square_\kappa(E)$ and let $\langle S_\alpha \mid \alpha \in E \rangle$ satisfy $\diamond_{\kappa^+}(E)$. We construct a κ^+ -Souslin tree, $\mathbf{T}$, by recursion on the levels, so that for each limit ordinal $\alpha < \kappa^+$, $\mathbf{T} \upharpoonright \alpha$ is an $(\alpha, |\alpha|^+)$ -tree. The elements of $\mathbf{T}$ will be members of κ , and we shall have $\alpha <_T \beta \rightarrow \alpha < \beta$. We set $T_0 = \{0\}$. If T_α is defined, $T_{\alpha+1}$ is obtained by appointing two new ordinals as extensions of each member of T_α . Suppose finally that $\lim(\alpha)$ and $\mathbf{T} \upharpoonright \alpha$ is defined. For each element x of $\mathbf{T} \upharpoonright \alpha$ we attempt to define an α -branch b_x^α of $\mathbf{T} \upharpoonright \alpha$, containing x , as follows.

Let $x \in \mathbf{T} \upharpoonright \alpha$ be given. Let $\langle \gamma_\nu \mid \nu < \lambda \rangle$ be the monotone enumeration of C_α . Let $\bar{\nu}(x)$ be the least ν such that $x \in T \upharpoonright \gamma_\nu$. Define a sequence $\langle p_\nu^x \mid \bar{\nu}(x) \leq \nu < \lambda \rangle$ of elements of $\mathbf{T} \upharpoonright \alpha$ as follows:

$p_{\bar{\nu}(x)}^x$ = the least (ordinalwise) $y \in T_{\gamma_{\bar{\nu}(x)}}$ such that $x \leq_T y$.

$p_{\nu+1}^x$ = the least $y \in T_{\gamma_{\nu+1}}$ such that $p_\nu^x \leq_T y$.

And if $\lim(\eta)$,

p_η^x = the unique $y \in T_{\gamma_\eta}$ such that for all $\nu < \eta$, $p_\nu^x \leq_T y$ (if it exists).

If the above definition breaks down (i.e. if p_η^x is undefined for some limit ordinal $\eta < \lambda$), then the entire construction breaks down. But for the meantime, let us assume that this sorry state of affairs does not arise, and describe how b_x^α is defined. Set $b_x^\alpha = \{y \in T \upharpoonright \alpha \mid \exists \nu < \lambda (y \leq_T p_\nu^x)\}$. Clearly, b_x^α is an α -branch of $T \upharpoonright \alpha$, containing x .

We define T_α as follows. If $\alpha \notin E$, let T_α consist of one-point extensions of each b_x^α for $x \in T \upharpoonright \alpha$. If $\alpha \in E$ and S_α is not a maximal antichain of $T \upharpoonright \alpha$, do likewise. Otherwise, let T_α consist of one-point extensions of each b_x^α such that x lies above an element of S_α .

That completes the definition of $\mathbf{T} = \bigcup_{\alpha < \kappa^+} T_\alpha$. Providing the definition of the p -sequence did not break down at any stage, $\mathbf{T}$ will clearly be a κ^+ -tree. We'll suppose that the definition of some p -sequence did break down. Let α be the least limit ordinal such that for some $x \in T \upharpoonright \alpha$, the sequence $\langle p_\nu^x \mid \bar{\nu}(x) \leq \nu < \lambda \rangle$ was not well-defined. Let $\eta < \lambda$ be the least (limit) ordinal such that p_η^x was not defined. Now, since $\lim(\eta)$, γ_η is a limit point of C_α , so $\gamma_\eta \notin E$ and $C_{\gamma_\eta} = \gamma_\eta \cap C_\alpha = \{\gamma_\nu \mid \nu < \eta\}$. Thus if we define $\langle q_\nu^x \mid \bar{\nu}(x) \leq \nu < \eta \rangle$ from γ_η as $\langle p_\nu^x \mid \bar{\nu}(x) \leq \nu < \lambda \rangle$ was defined from α , then for all $\nu < \eta$, $q_\nu^x = p_\nu^x$. But look, $\langle q_\nu^x \mid \bar{\nu}(x) \leq \nu < \eta \rangle$ determined the γ_η -branch $b_{x_\eta}^{\gamma_\eta}$, and since $\gamma_\eta \notin E$, this branch has an extension on T_{γ_η} . Hence the sequence $\langle p_\nu^x \mid \bar{\nu}(x) \leq \nu < \eta \rangle$ has an extension of T_{γ_η} . Thus p_η^x is defined, a contradiction. Hence $\mathbf{T}$ is a well-defined κ^+ -tree, as required.

We claim that $\mathbf{T}$ is Souslin. Suppose otherwise. Let A be a maximal antichain of T of cardinality κ^+ . Set $C = \{\alpha \in \kappa^+ \mid T \upharpoonright \alpha \subseteq \alpha \text{ \& } A \cap \alpha \text{ is a maximal antichain of } T \upharpoonright \alpha\}$, a closed unbounded subset of κ^+ . Pick $\alpha \in C \cap E$ such that $A \cap \alpha = S_\alpha$. Then T_α was constructed so that every element of T_α lies above an element of $A \cap \alpha$. Hence $A \cap \alpha$ is a maximal antichain in $\mathbf{T}$. Hence $A = A \cap \alpha$, which is absurd. Hence $\mathbf{T}$ is Souslin. $\square$

REMARK. By a combinatorial argument, one can show that in the presence of GCH, $\square_\kappa$ implies that there is a stationary set $E \subseteq \kappa^+$ for which $\square_\kappa(E)$ and $\diamond_{\kappa^+}(E)$ hold. Hence $\text{GCH} + \square_\kappa$ is already strong enough to yield $\neg \text{SH}(\kappa^+)$. The details of all of this (which followed some observations of Gregory) will be given in the forthcoming revised edition of *DEVLIN* [1973].

12. The fine structure of the constructible hierarchy

The deeper results about the constructible universe, and in particular the proof of the combinatorial principle $\square_\kappa$, depend² upon a detailed study of

² See footnote 5.

the levels of the constructible hierarchy. This study, due to Jensen, is exceedingly technical, and in general it is not necessary to be familiar with all the details in order to apply the results yielded by the theory. We shall therefore content ourselves here with a brief description of the theory, and refer the reader to DEVLIN [1973] for further details. (Actually, for technical reasons, the development in DEVLIN [1973] is carried out not for the constructible hierarchy as we have defined it here, but for a slightly modified hierarchy. However, the proofs can all be modified to cover the usual hierarchy, so we shall give our description here for the usual hierarchy.)

Basically, the idea behind the fine structure theory is this. We have seen that the constructible hierarchy is Σ_1^{ZF} and uniformly Σ_1^{ZF} for limit $\alpha > \omega$, that Σ_1 -submodels of any limit L_α are isomorphic to limit levels of the hierarchy itself, and that limit L_α 's ($\alpha > \omega$) have uniformly Σ_1^{ZF} Σ_1 Skolem functions. Thus, we can carry out condensation arguments, etc. in a uniform manner in order to obtain results about Σ_1 predicates over the hierarchy. To carry out analogous arguments for Σ_n predicates is, in general, not possible. For example, although it is possible to construct " Σ_n Skolem functions" for limit L_α 's ($\alpha > \omega$), they tend to be rather complicated objects, and certainly not uniformly defined. But it is not hard to see that many of our nice, uniform results about limit L_α 's and Σ_1 predicates on them carry through virtually unchanged for structures of the form $\langle L_\alpha, A \rangle$, where $\text{lim}(\alpha)$, $\alpha > \omega$, and $\gamma < \alpha \rightarrow A \cap L_\gamma \in L_\alpha$ (such $\langle L_\alpha, A \rangle$ are said to be *amenable*). What we do in the fine structure theory, is to show that, for instance, a Σ_n predicate on some limit L_α is "equivalent" (in some uniform manner) to a Σ_1 predicate on some amenable $\langle L_\alpha, A \rangle$. We then work with this structure.

The notion of amenability comes in as follows. If φ is a Σ_0 sentence of $\mathcal{L}_{L_\alpha}(A)$ (the language $\mathcal{L}_{L_\alpha}$ with the additional unary predicate $\dot{A}$ to denote A), then

$$\models_{\langle L_\alpha, A \rangle} \varphi \quad \text{iff} \quad \models_{\langle \text{TC}(\text{ran}(\varphi)), A \cap \text{TC}(\text{ran}(\varphi)) \rangle} \varphi.$$

And, if $\langle L_\alpha, A \rangle$ is amenable, then for all φ , $A \cap \text{TC}(\text{ran}(\varphi)) \in L_\alpha$. Hence, by a straightforward generalisation of the arguments used to prove 8.4 and 8.5, we have:

12.1. LEMMA. $\models_{\langle L_\alpha, A \rangle}^{\Sigma_1}$ is uniformly $\Sigma_1^{(L_\alpha, A)}$ for amenable $\langle L_\alpha, A \rangle$.

The notion of a Σ_1 Skolem function for amenable structures $\langle L_\alpha, A \rangle$ is

defined much as in Section 8, and analogues of 8.1–8.3 clearly hold in this context. Moreover, by an argument as in 8.6, we have:

12.2. LEMMA. *Let $\langle L_\alpha, A \rangle$ be amenable. Then $\langle L_\alpha, A \rangle$ has a uniformly $\Sigma_1^{(L_\alpha, A)} \Sigma_1$ Skolem function.*

We denote the canonical Σ_1 Skolem function for $\langle L_\alpha, A \rangle$ by $h_{\alpha, A}$, and let³ H_i be the canonical Σ_0 formula of $\mathcal{L}(A)$ such that $y = h_{\alpha, A}(i, x) \leftrightarrow \exists z \in L_\alpha [\models_{(L_\alpha, A)} H_i(\bar{z}, \bar{y}, \bar{x})]$ for any amenable $\langle L_\alpha, A \rangle$. As in Section 8, $\langle H_i \mid i < \omega \rangle$ is recursive, and $H_{\alpha, A}$ is uniformly $\Sigma_1^{(L_\alpha, A)}$ (for amenable $\langle L_\alpha, A \rangle$ where $H_{\alpha, A}(z, y, i, x) \leftrightarrow [\models_{(L_\alpha, A)} H_i(\bar{z}, \bar{y}, \bar{x})]$).

Let $\alpha > \omega$, $n > 0$. The Σ_n -projectum of α , ρ_α^n , is the smallest $\rho \leq \alpha$ such that there is a $\Sigma_n(L_\alpha)$ map f with $f''L_\rho = L_\alpha$.

It can be shown that ρ_α^n is equal to the largest $\rho \leq \alpha$ such that $\langle L_\rho, A \rangle$ is amenable for all $A \in \Sigma_n(L_\alpha) \cap \mathcal{P}(L_\rho)$, and also equal to the smallest ρ such that $\mathcal{P}(\rho) \cap \Sigma_n(L_\alpha) \not\subseteq L_\alpha$.

It is easily seen that $m < n \rightarrow \rho_\alpha^m \leq \rho_\alpha^n$. Hence we set $\rho_\alpha^0 = \alpha$ for all α .

For each $\alpha > \omega$, each $n \geq 0$, we can associate with α a *standard code* A_α^n and a *standard parameter* p_α^n , with the following properties:

- (i) $A_\alpha^n \subseteq L_{\rho_\alpha^n}$ and $A_\alpha^n \in \Sigma_n(L_\alpha)$.
- (ii) $A_\alpha^0 = p_\alpha^0 = \emptyset$.
- (iii) For all $m > 0$, $\Sigma_m(\langle L_{\rho_\alpha^n}, A_\alpha^n \rangle) = \mathcal{P}(L_{\rho_\alpha^n}) \cap \Sigma_{n+m}(L_\alpha)$.
- (iv) Suppose $\alpha > \omega$, $m \geq 0$, $n \geq 1$, $\langle L_{\bar{\rho}}, \bar{A} \rangle$ is amenable, and

$$\pi : \langle L_{\bar{\rho}}, \bar{A} \rangle <_{\Sigma_m} \langle L_{\rho_\alpha^n}, A_\alpha^n \rangle.$$

Then there is a unique $\bar{\alpha} \geq \bar{\rho}$ such that $\bar{\rho} = \rho_{\bar{\alpha}}^n$, $\bar{A} = A_{\bar{\alpha}}^n$. Moreover, there is a unique $\bar{\pi} \supseteq \pi$, $\bar{\pi} : L_{\bar{\alpha}} <_{\Sigma_{m+n}} L_\alpha$, such that for all $i \leq n$:

- (a) $\bar{\pi}(p_{\bar{\alpha}}^i) = p_\alpha^i$;
- (b) $(\bar{\pi} \upharpoonright L_{\rho_{\bar{\alpha}}^i}) : \langle L_{\rho_{\bar{\alpha}}^i}, A_{\bar{\alpha}}^i \rangle <_{\Sigma_{m+n-i}} \langle L_{\rho_\alpha^i}, A_\alpha^i \rangle$.

Notice that (for $n > 0$) by the definition of ρ_α^n , any $\Sigma_n(L_\alpha)$ predicate on L_α is reducible to a $\Sigma_n(L_\alpha)$ predicate on $L_{\rho_\alpha^n}$. Hence, by condition (iii) above, any $\Sigma_n(L_\alpha)$ predicate on L_α can be coded as a $\Sigma_1(\langle L_{\rho_\alpha^n}, A_\alpha^n \rangle)$ predicate on $L_{\rho_\alpha^n}$. And by condition (iv), we can carry out condensation arguments on structures of this latter form, using our uniform Σ_1 Skolem functions $h_{\alpha, A}$ defined above.

³ Of course, we have already used the same symbols H_i in the case of the Skolem functions h_α . However, there should be no cause for confusion in our notation. Indeed, h_α is the same as $h_{\alpha, \emptyset}$, so our new usage can be regarded as an extension of the previous one, with the predicates H_α being a special case of the predicates $H_{\alpha, A}$.

13. The combinatorial principle $\square_\kappa$

The aim of this section is to prove 11.1. First of all, we remove the complication of having to consider the stationary set E involved in 11.1.

For the whole of this section, κ will denote a fixed infinite cardinal. Since $\square_\kappa$ is trivially true (in ZFC) for $\kappa = \omega$, we shall also assume that κ is uncountable. (This is, in any case, the result required for applications.)

13.1. LEMMA. *Assume $\square_\kappa$. Then there is a stationary set $E \subseteq \kappa^+$ such that $\alpha \in E \rightarrow \text{cf}(\alpha) = \omega$ and $\square_\kappa(E)$ holds.*

PROOF. Let $\langle A_\lambda \mid \lambda < \kappa^+ \ \& \ \text{lim}(\lambda) \rangle$ be a $\square_\kappa$ -sequence. Let B_λ be the set of limit points of A_λ for each λ . The B -sequence has the following properties:

- (i) B_λ is a closed subset of λ ;
- (ii) $\text{cf}(\lambda) > \omega \rightarrow B_\lambda$ is unbounded in λ ;
- (iii) $\gamma \in B_\lambda \rightarrow B_\gamma = \gamma \cap B_\lambda$;
- (iv) $\text{cf}(\lambda) < \kappa \rightarrow |B_\lambda| < \kappa$.

Since $\text{cf}(\lambda) = \omega \rightarrow \text{otp}(B_\lambda) < \kappa$, we can define a partition $W = \bigcup_{\nu < \kappa} W_\nu$ of the set $W = \{\alpha \in \kappa^+ \mid \text{cf}(\alpha) = \omega\}$ by setting $W_\nu = \{\lambda \in W \mid \text{otp}(B_\lambda) = \nu\}$. Since W is stationary in κ^+ , we can pick $\nu_0 < \kappa$ such that W_{ν_0} is stationary. Set $E = W_{\nu_0}$. We show that $\square_\kappa(E)$ holds.

Define $\langle D_\lambda \mid \lambda < \kappa^+ \ \& \ \text{lim}(\lambda) \rangle$ by:

$$D_\lambda = \begin{cases} B_\lambda & \text{if } \text{otp}(B_\lambda) \leq \nu_0, \\ B_\lambda - \{\alpha \in B_\lambda \mid \text{otp}(B_\alpha) \leq \nu_0\} & \text{otherwise.} \end{cases}$$

It is easily seen that the D -sequence has properties (i)–(iv) above. And clearly, $D_\lambda \cap E = \emptyset$ for each λ .

Define $\langle C_\lambda \mid \lambda < \kappa^+ \ \& \ \text{lim}(\lambda) \rangle$ by recursion, thus:

$$C_\lambda = \begin{cases} \bigcup \{C_\gamma \mid \gamma \in D_\lambda\} & \text{if } \text{sup}(D_\lambda) = \lambda, \\ \bigcup \{C_\gamma \mid \gamma \in D_\lambda\} \cup \{\alpha_n \mid n < \omega\} & \text{otherwise,} \end{cases}$$

where $\langle \alpha_n \mid n < \omega \rangle$ is any ω -sequence cofinal in λ with $\alpha_0 = \text{sup}(D_\lambda)$.

It is easily seen that the C -sequence is a $\square_\kappa$ -sequence and that D_λ is the set of limit points of C_λ for each λ . Hence the C -sequence is a $\square_\kappa(E)$ -sequence. $\square$

Notice that in the course of the above proof we effectively established the following result:

13.2. LEMMA. $\square_\kappa$ is equivalent to the existence of a sequence $\langle B_\lambda \mid \lambda < \kappa^+ \ \& \ \text{lim}(\lambda) \rangle$ satisfying conditions (i)–(iv) of the above proof.

13.2 gives the form of $\square_\kappa$ which is perhaps more often seen in the literature.

Set

$$S = \{\alpha \mid \kappa < \alpha < \kappa^+ \ \& \ \text{lim}(\alpha) \ \& \ \models_{L_\alpha} \text{“}\kappa \text{ is the largest cardinal”}\}.$$

It suffices to prove the following result: there is a sequence $\langle C_\alpha \mid \alpha \in S \rangle$ such that:

- (i) C_α is a closed unbounded subset of α ;
 - (ii) $\text{otp}(C_\alpha) \leq \kappa$;
 - (iii) if γ is a limit point of C_α , then $\gamma \in S$ and $C_\gamma = \gamma \cap C_\alpha$.
- To obtain $\square_\kappa$ from this result, we argue as follows. Let C_α^0 be the set of limit points of C_α . Identifying the closed unbounded set S with κ^+ , we have:
- (i) C_α^0 is a closed subset of α ;
 - (ii) if $\text{cf}(\alpha) > \omega$, then C_α^0 is unbounded in α ;
 - (iii) $\text{otp}(C_\alpha^0) \leq \kappa$;
 - (iv) if $\gamma \in C_\alpha^0$, then $C_\gamma^0 = \gamma \cap C_\alpha^0$.

If κ is regular, then (iii) gives: $\text{cf}(\alpha) < \kappa \rightarrow |C_\alpha^0| < \kappa$, so we are done by 13.2. Otherwise, set $\bar{\kappa} = \text{cf}(\kappa) < \kappa$, let $\langle \theta_\nu \mid \nu < \bar{\kappa} \rangle$ be a normal sequence of limit ordinals cofinal in κ , and proceed as follows.

Set $\theta_{\bar{\kappa}} = \kappa$ for convenience. Assume further that $\theta_0 = 0$, $\theta_1 = \omega$. If $\theta_\nu < \text{otp}(C_\alpha^0) \leq \theta_{\nu+1}$, set $C_\alpha^1 = \{\gamma \in C_\alpha^0 \mid \text{otp}(\gamma \cap C_\alpha^0) \geq \theta_\nu\}$. If no such ν exists, then $\text{otp}(C_\alpha^0) = \theta_\nu$ for some limit ordinal $\nu \leq \bar{\kappa}$, and we can set $C_\alpha^1 = \{\gamma \in C_\alpha^0 \mid \exists \tau < \nu [\text{otp}(\gamma \cap C_\alpha^0) = \theta_\tau]\}$. Then $\langle C_\alpha^1 \mid \alpha < \kappa^+ \ \& \ \text{lim}(\alpha) \rangle$ satisfies the requirements of 13.2, so again we are done.

In order to establish the existence of the sequence $\langle C_\alpha \mid \alpha \in S \rangle$ as above, we require the fine structure theory of the previous section. We assume $V = L$ from now on.^{4,5}

⁴ Proofs using the fine-structure tend to be rather long and tedious, and the present case is no exception. We shall therefore omit most of the individual verifications, and try instead to cover the main line of the argument. This will still be fairly heavy going. We have included this sketch in this otherwise fairly easy-going account of L because we felt that, as fine-structure arguments play an extremely dominant role in present day constructibility theory, some idea of what is involved should be provided. Readers who do not wish to know the gory details can skip the rest of this section without affecting the reading of later parts of the article.

⁵ Actually, Silver has shown that the full power of the fine-structure theory is not required in order to prove $\square_\kappa$. He observes that all we require is a functional hierarchy which resembles (to some extent) the hierarchy of the Skolem functions $h_{\alpha, \lambda}$ used in the proof of $\square_\kappa$ presented here. The point being that in order to obtain such a hierarchy with sufficient properties to

Let α, β be ordinals, $\alpha \leq \beta$. We say α is *regular at β* iff there is no L_β -definable map of a bounded subset of α cofinally into α . For n a positive integer, we say α is Σ_n -*regular at β* iff there is no $\Sigma_n(L_\beta)$ map of a bounded subset of α cofinally into α . For $\alpha \in S$, we define:

$\beta(\alpha)$ = the least β such that α is not regular at β .

$n(\alpha)$ = the least n such that α is not Σ_n -regular at $\beta(\alpha)$.

$\rho(\alpha) = \rho_{\beta(\alpha)}^{n(\alpha)-1}$; $A(\alpha) = A_{\beta(\alpha)}^{n(\alpha)-1}$.

Notice that, as α is $\Sigma_{n(\alpha)-1}$ -regular at $\beta(\alpha)$ but not $\Sigma_{n(\alpha)}$ -regular at $\beta(\alpha)$, we have $\rho_{\beta(\alpha)}^{n(\alpha)} \leq \alpha \leq \rho(\alpha)$ for all $\alpha \in S$. In fact, it is not too hard to show that $\rho_{\beta(\alpha)}^{n(\alpha)} = \kappa$ for all $\alpha \in S$, a fact we shall use during the proof.

We now partition S into two classes by setting: $P = \{\alpha \in S \mid n(\alpha) = 1 \ \& \ \text{succ}(\beta(\alpha))\}$, $R = S - P$. The definition of C_α will depend upon whether $\alpha \in P$ or $\alpha \in R$. In fact, if $\alpha \in P$, the definition of C_α is extremely easy. For if $\alpha \in P$, then $\text{cf}(\alpha) = \omega$, and we can take for C_α any ω -sequence cofinal in α . (Since C_α will have no limit points in this case, there is nothing more to worry about.) That $\alpha \in P \rightarrow \text{cf}(\alpha) = \omega$ is easily seen. There is a $\Sigma_1(L_\beta)$ map of a bounded subset of α cofinally into α . Taking some canonical Σ_1 representation of this mapping, the existential quantifier ranges over the definable subsets of L_γ , where $\beta = \gamma + 1$. For each fixed formula of $\mathcal{L}$, we can obtain a "part" of this function by regarding the fixed formula as providing the solution to the existential quantifier, letting the parameters concerned run over L_γ . But this "part" of the function is clearly L_γ -definable, so as $\gamma < \beta$, it cannot be cofinal in α . Since the union of the countably many "part" functions obtained as above is a function which is cofinal in α , we conclude that $\text{cf}(\alpha) = \omega$.

Suppose now that $\alpha \in R$. Set $\beta = \beta(\alpha)$, $n = n(\alpha)$, $\rho = \rho(\alpha)$, $A = A(\alpha)$. Since either $n > 1$ or else $\lim(\beta)$, we always have $\lim(\rho)$. Set $h = h_{\rho, A}$. Since

obtain $\square_\kappa$, only "elementary considerations" are necessary. (Silver calls his hierarchy a "machine".) Silver's method not only proves $\square_\kappa$, but also all of the best known consequences of the fine-structure theory. And though still fairly long, it avoids a great deal of the proof by cases involved in fine-structure derivations. Moreover, as we mentioned earlier, it can be developed using only standard facts about L , such as were considered in the first few sections of this paper. For these reasons, the Silver approach is undoubtedly superior to the standard fine-structure proofs, when all that one requires is the simplest and quickest rigorous proof of, say, $\square_\kappa$ assuming only standard, well-known facts about L . The main drawback is that the "L-machine" has a somewhat ad hoc structure, without the simple intuitive motivation of the fine-structure theory. (Also, the Silver method is not well suited to the more complex fine-structure results, such as the construction of high gap morasses.) For this reason we have chosen to outline the fine-structure proof here. A similar account of Silver's method would, we feel, be much less clear. Nevertheless, for the reader who would like to see a relatively quick, rigorous proof of $\square_\kappa$, we recommend the Silver approach. At the time of writing this article, Silver's proof is not available in the literature, but an account of it will certainly be included in the forthcoming revised edition of DEVLIN [1973].

$\rho_\beta^n = \kappa$, we may let $p = p(\alpha) =$ the $<_L$ -least $p \in L_\rho$ such that $L_\rho = h''(\omega \times (\kappa \times \{p\}))$, and such that $\alpha = (p)_0$ in case $\alpha < \rho$, as well.

For $\tau \leq \rho$, define h_τ by

$$y = h_\tau(i, x) \leftrightarrow y, x \in L_\tau \ \& \ \exists z \in L_\tau [\models_{(L_\rho, A)} H_i(z, y, x)].$$

Clearly, $h_\tau = h_{\tau, A \cap L_\tau}$ for all amenable $\langle L_\tau, A \cap L_\tau \rangle$.

Define a map g from a subset of κ onto α by: $g(\omega\nu + i) = h(i, \langle \nu, p \rangle)$, if this value is defined and lies in α , with g otherwise undefined. Clearly, g has a uniformly Σ_1 -definition of the form:

$$\tau = g(\nu) \leftrightarrow (\exists z \in L_\rho) G(z, \tau, \nu),$$

where G is $\Sigma_0^{(L_\rho, A)}(\{p\})$ (uniformly). For $X \subseteq L_\rho$, set $\alpha_X = \sup(\alpha \cap X)$.

Define functions $k : \theta \rightarrow \kappa$, $l : \theta \rightarrow \alpha$, $m : \theta \rightarrow \rho$, for some $\theta \leq \kappa$, by a simultaneous recursion, as follows.

$k(\nu) =$ the least $\tau \in \text{dom}(g)$ such that $g(\tau) > l(\nu)$ and $|l(\nu)|^{L_{g(\tau)}} \leq \kappa$.

$l(\nu) = \alpha_{X_\nu}$, where $X_\nu = h''_{m(\nu)}(\omega \times (\kappa \times \{p\}))$.

$m(0) = \max(\kappa, \eta + 1)$, where η is the least ordinal such that $p \in L_{\eta+1}$.

$m(\lambda) = \sup_{\nu < \lambda} m(\nu)$, if $\lambda < \rho$ (otherwise undefined), for $\lim(\lambda)$.

$m(\nu + 1) =$ the least $\gamma > m(\nu)$ such that $g \circ k(\nu) < \gamma$ and $A \cap L_{m(\nu)} \in L_\gamma$ and

$$l(\nu), m(\nu) \in h''_\gamma(\omega \times (\kappa \times \{p\})), \quad \exists z \in L_\gamma G(z, g \circ k(\nu), k(\nu)).$$

It is easily seen that the above recursion only breaks down when, for some limit ordinal $\theta \leq \kappa$, $\sup_{\nu < \theta} m(\nu) = \rho$. It follows that $\langle l(\nu) \mid \nu < \theta \rangle$ is a normal sequence, cofinal in α .

Set $C_\alpha = \{l(\nu) \mid \nu < \theta\}$. Notice that $\text{otp}(C_\alpha) = \theta \leq \kappa$. We must show that, if $\bar{\alpha}$ is a limit point of C_α , then $\bar{\alpha} \in R$ and $C_{\bar{\alpha}} = \bar{\alpha} \cap C_\alpha$. (We must show that $\bar{\alpha} \in R$, rather than just $\bar{\alpha} \in S$, because of the somewhat arbitrary way we defined C_λ for $\lambda \in P$.)

Let $\bar{\alpha} < \alpha$ be a limit point of C_α . Pick $\lambda < \theta$ with $\bar{\alpha} = l(\lambda)$. Thus $l(\lambda) = \sup_{\nu < \lambda} l(\nu)$. By means of the definition of k , it is not hard to show that $\bar{\alpha} \in S$. (We have $l(\nu) < g \circ k(\nu) < l(\nu + 1)$ for all ν .) The rest of the proof is essentially a condensation argument.

To commence, we notice that $\bar{\alpha} \subseteq X_\lambda$. This is because $\kappa \subseteq X_\lambda$ and $\nu < \lambda \rightarrow |\alpha_{X_\nu}|^{L_{m(\nu)}} \leq \kappa$. So, letting $\pi : \langle L_{\bar{\rho}}, \bar{A} \rangle \cong \langle X_\lambda, A \cap X_\lambda \rangle$, we have

$$\pi : \langle L_{\bar{\rho}}, \bar{A} \rangle <_{\Sigma_1} \langle L_{m(\lambda)}, A \cap L_{m(\lambda)} \rangle, \quad \pi \restriction \bar{\alpha} = \text{id} \restriction \bar{\alpha}.$$

Since we also have (trivially) $\pi : \langle L_{\bar{\rho}}, \bar{A} \rangle <_{\Sigma_0} \langle L_\rho, A \rangle$, there are unique $\bar{\beta}, \bar{\pi}$ such that $\bar{\rho} = \rho_{\bar{\beta}}^{n-1}$, $\bar{A} = A_{\bar{\beta}}^{n-1}$, $\bar{\pi} \supseteq \pi$, and $\bar{\pi} : L_{\bar{\beta}} <_{\Sigma_1} L_\rho$ (at least). Set

$\bar{p} = \pi^{-1}(p)$. Since $\pi \restriction \bar{\alpha} = \text{id} \restriction \bar{\alpha}$, $\bar{\pi}(\bar{\alpha}) = \alpha$. Hence $\bar{\alpha} < \bar{p} \rightarrow \bar{\alpha} = (\bar{p})_0$. Let $\bar{h} = h_{\bar{p}, \bar{\alpha}}$. Clearly, $\bar{h} = \pi^{-1} \circ h_{m(\lambda)} \circ \pi$.

It is now just a routine (but by no means easy!) matter to show (using the fact that $\bar{\pi} : L_{\bar{\beta}} <_{\Sigma_1} L_{\beta}$, etc.) that $\rho_{\bar{\beta}}^{\bar{\pi}} = \kappa$, $\bar{\beta} = \beta(\bar{\alpha})$, $n = n(\bar{\alpha})$, $\bar{p} = p(\bar{\alpha})$. In particular, $\bar{\alpha} \in R$. It follows that if $\bar{g}, \bar{k}, \bar{l}, \bar{m}$ are defined from $\bar{\alpha}$ as g, k, l, m were defined from α , then for all $\nu < \lambda$, $\bar{\pi}(\bar{g}(\nu)) = g(\nu)$, $\bar{\pi}(\bar{k}(\nu)) = k(\nu)$, $\bar{\pi}(\bar{l}(\nu)) = l(\nu)$, $\bar{\pi}(\bar{m}(\nu)) = m(\nu)$. In particular, since $\bar{\pi} \restriction \bar{\alpha} = \text{id} \restriction \bar{\alpha}$, $C_{\bar{\alpha}} = \bar{\alpha} \cap C_{\alpha}$, as required.

It is precisely in order to establish the various facts involved here that the definition of the function m , in particular, was as complicated as it was. The key, initial step is to define a map g' over $\langle L_{m(\lambda)}, A \cap L_{m(\lambda)} \rangle$ using the predicate G . Since $\pi^{-1} g' = g$ and $k''\lambda \subseteq \text{dom}(g')$, g' is thus a $\Sigma_1^{(L_{\bar{\beta}}, A)}(\{\bar{p}\})$ map of a subset of κ cofinally into $\bar{\alpha}$. The required equalities now follow by virtue of the canonical way the various parameters were defined. (The function g' turns out to be $\bar{g}$.) We omit any further details, since it should be clear by now that the whole thing is really just a condensation argument. (In this, and other respects, the proof is typical of fine structure proofs.)

14. Weakly compact cardinals in L

See Section 7 and 6.10 in Chapter B.3 for background on weakly compact cardinals. Using the fine structure theory, it is possible to obtain useful characterisations of the weakly compact cardinals in L. Firstly, by a modification of the proof of $\square_{\kappa}$ outlined above, we have:

14.1. THEOREM (Jensen). *Assume $V = L$. Let κ be an uncountable regular cardinal, not weakly compact. Then there is a stationary set $E \subseteq \kappa$ and a sequence $\langle C_{\lambda} \mid \lambda < \kappa \text{ \& } \lim(\lambda) \rangle$ such that:*

- (i) C_{λ} is closed and unbounded in λ ;
- (ii) if $\gamma < \lambda$ is a limit point of C_{λ} , then $\gamma \notin E$ and $C_{\gamma} = \gamma \cap C_{\lambda}$.

The assumption that κ be not weakly compact in the above is clearly necessary, since a simple argument (in ZFC) shows that if κ is weakly compact, and if $E \subseteq \kappa$ is stationary in κ , then $E \cap \lambda$ is stationary in λ for some regular cardinal $\lambda < \kappa$ (see Theorem 7.3 of Chapter B.3). (Hence no such sequence $\langle C_{\lambda} \mid \lambda < \kappa \text{ \& } \lim(\lambda) \rangle$ as above can exist.) These remarks provide us with our first characterisation.

14.2. THEOREM (Jensen). *Assume $V = L$. An uncountable regular cardinal*

κ is weakly compact iff: whenever $E \subseteq \kappa$ is stationary in κ , there is a limit ordinal $\lambda < \kappa$ such that $E \cap \lambda$ is stationary in λ .

By a forcing argument, Kunen has shown that the assumption of $V = L$ in the above is necessary (By which we mean that $ZFC + GCH$ is not enough.)

Using 14.1, a virtual repetition of the proof of 11.3 yields:

14.3. THEOREM (Jensen). Assume $V = L$. If κ is an uncountable regular cardinal which is not weakly compact, then there is a κ -Souslin tree. Hence (since the weak compactness of κ implies that there are no κ -Aronszajn trees) an uncountable regular cardinal κ is weakly compact iff there are no κ -Souslin trees.

Using 14.3, it is possible to obtain various other equivalences of weak compactness in L . We shall give three such, all in the field of infinitary combinatorics.

As usual, if X is a set, $[X]^n$ denotes the collection of all n -element subsets of X . We write $\kappa \rightarrow (\lambda)_\mu^n$ iff whenever $f: [\kappa]^n \rightarrow \mu$, there is a set $X \subseteq \kappa$, $|X| = \lambda$, such that $|f''[X]^n| = 1$. (We say X is *homogeneous* for the partition f .) A well-known theorem of ZFC (6.10 in Chapter B.3) is:

14.4. THEOREM. An uncountable cardinal κ is weakly compact iff $\kappa \rightarrow (\kappa)_2^2$ iff $\forall n < \omega \forall \mu < \kappa [\kappa \rightarrow (\kappa)_\mu^n]$.

Write $\kappa \rightarrow [\lambda]_{\mu, \theta}^n$ iff whenever $f: [\kappa]^n \rightarrow \mu$, there is $X \subseteq \kappa$, $|X| = \lambda$, such that $|f''[X]^n| \leq \theta$. Clearly, if κ is weakly compact, then $\kappa \rightarrow [\kappa]_{\mu, \theta}^n$ for all $\mu, \theta < \kappa$.

14.5. THEOREM (Martin; Shore). Assume $V = L$. A regular uncountable cardinal κ is weakly compact iff $\kappa \rightarrow [\kappa]_{\mu, \theta}^n$ holds for some/all $n \geq 2$, $0 < \theta < \mu < \kappa$.

PROOF. Let T be a κ -Souslin tree. Let $0 < \theta < \mu < \kappa$ be given. It suffices to show that the property $\kappa \rightarrow [\kappa]_{\mu, \theta}^2$ fails. We may assume that various levels of T have been discarded, so that each member of T has at least μ immediate successors. Let $S(x)$ denote the set of immediate successors of x , each $x \in T$. Let $f^*: [S(x)]^2 \rightarrow \mu - \{0\}$, each $x \in T$, where none of the resulting partition classes are empty. Define $f: [T]^2 \rightarrow \mu$ as follows: If

$y_0, y_1 \in T$ are comparable, set $f(\{y_0, y_1\}) = 0$. Otherwise, let x be the greatest common predecessor of y_0, y_1 . Pick $x_i \in S(x)$ with $x_i \leq_T y_i$. Set $f(\{y_0, y_1\}) = f^x(\{x_0, x_1\})$.

Suppose that for some $X \subseteq T$, $|X| = \kappa$, $A = f''[X]^2$ has cardinality at most θ . Since T has no antichain of size κ , we know that $0 \in A$. Let Y be the set of all elements of T which lie in X or else below some element of X . Then $f''[Y]^2 = A$, of course. Hence, for each $y \in Y$, there is an immediate successor of y which is not in Y . The set of all such is clearly an antichain of T , which is absurd, since $|Y| = \kappa$. Hence f testifies the failure of $\kappa \rightarrow [\kappa]_{\mu, \theta}^2$. $\square$

A mapping $f: [\kappa]^n \rightarrow \kappa$ is said to be a *set-mapping* if $f(\sigma) \notin \sigma$ for all $\sigma \in [\kappa]^n$. A set $X \subseteq \kappa$ is said to be *free* for the set mapping $f: [\kappa]^n \rightarrow \kappa$ if $f''[X]^n \cap X = \emptyset$. We write $(\kappa, n) \rightarrow \lambda$ iff every set-mapping $f: [\kappa]^n \rightarrow \kappa$ has a free set of size λ . An old result of Erdős-Hajnal is: if κ is weakly compact, then $(\kappa, n) \rightarrow \kappa$ for all $n \in \omega$. The proof is quite easy. Let $f: [\kappa]^n \rightarrow \kappa$ be a set-mapping. Define a partition $g: [\kappa]^{n+1} \rightarrow n+2$ by: for $x_1 < \dots < x_{n+1} < \kappa$,

$$g(\{x_1, \dots, x_{n+1}\}) = \begin{cases} i & \text{where } i \text{ is least with } f(\{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{n+1}\}) \\ & = x_i, \text{ if such an } i \text{ exists;} \\ 0 & \text{otherwise.} \end{cases}$$

Let $X \subseteq \kappa$, $|X| = \kappa$, be homogeneous for g . Clearly, $g''[X]^{n+1} = \{0\}$ (since f is a function). Hence X is free for f .

14.6. THEOREM (Devlin). *Assume $V = L$. A regular uncountable cardinal κ is weakly compact iff $(\kappa, 2) \rightarrow \kappa$ iff $\forall n \in \omega [(\kappa, n) \rightarrow \kappa]$.*

PROOF. Let T be a κ -Souslin tree. Define $f: [T]^2 \rightarrow T$ by

$$f(\{x, y\}) = \begin{cases} \text{the largest common predecessor of } x, y \text{ if } x \text{ and } y \text{ are not} \\ \text{comparable in } T. & \\ \text{an arbitrary element of } T - \{x, y\} & \text{otherwise.} \end{cases}$$

Suppose $X \subseteq T$ is free for the set-mapping f on T . Then, for each $x \in X$, there is clearly an immediate successor x' of x such that $\forall y \in T (x' \leq_T y \rightarrow y \notin X)$. Thus $\{x' \mid x \in X\}$ is an antichain of T . Thus $|X| < \kappa$. Hence f testifies the failure of $(\kappa, 2) \rightarrow \kappa$. The theorem follows immediately. $\square$

The above two examples were really results about Souslin trees, of course, rather than $V = L$. This is not the case with our next result.

A *graph* is a structure $\mathcal{G} = \langle G, E \rangle$, where G is a non-empty set and E is a collection of pairs from G , called the *edges* of $\mathcal{G}$. (If $\{x, y\} \in E$, we say x and y are *joined* in $\mathcal{G}$.) A *subgraph* of $\mathcal{G}$ is a substructure of $\mathcal{G}$ in the normal sense. If $H \subseteq G$, $\mathcal{G} \upharpoonright H$ denotes the subgraph of $\mathcal{G}$ with domain H . $\mathcal{G} \upharpoonright H$ is *small* if $|H| < |G|$.

Let $\mathcal{G} = \langle G, E \rangle$ be a graph, μ a cardinal. A mapping $h : G \rightarrow \mu$ is a μ -colouring if $h(x) = h(y) \rightarrow \{x, y\} \notin E$. The least μ such that $\mathcal{G}$ has a μ -colouring is called the *chromatic number* of $\mathcal{G}$, $\text{ch}(\mathcal{G})$. Thus $\text{ch}(\mathcal{G})$ is the smallest number of colours necessary to colour G , so that no two joined vertices have the same colour.

By $P(\kappa)$, let us mean the assertion that if $\mathcal{G}$ is a graph of cardinality κ , all of whose small subgraphs have countable chromatic number, then $\text{ch}(\mathcal{G})$ is countable. It is easily seen that $P(\kappa)$ holds whenever κ is weakly compact.

14.7. THEOREM (Shelah). *Assume $V = L$. Let $\kappa > \omega_1$ be a regular cardinal. Then $P(\kappa)$ holds iff κ is weakly compact.*

PROOF. Let $\kappa > \omega_1$ be regular but not weakly compact. By 14.1, there is a stationary set $S \subseteq \kappa$, $\alpha \in S \rightarrow \text{cf}(\alpha) = \omega$, such that $S \cap \lambda$ is not stationary in λ for any limit ordinal $\lambda < \kappa$. (Although we did not state it explicitly in 14.1, the “indicated” proof yields a stationary set of limit ordinals cofinal with ω .) We may assume that $\beta < \alpha \rightarrow \beta + \omega < \alpha$ for all $\alpha \in S$. And by $\Diamond_\kappa$, there is a partition $\langle B_n^\alpha \mid n < \omega \rangle$ of α , each $\alpha < \kappa$, such that whenever $\langle B_n \mid n < \omega \rangle$ is a partition of κ , the set

$$\{\alpha \in \kappa \mid \text{cf}(\alpha) = \omega \ \& \ \forall n \in \omega (B_n \cap \alpha = B_n^\alpha)\}$$

is stationary in κ .

For $\alpha \in S$, let A_α be a cofinal ω -sequence in α , chosen so that $\forall n [B_n^\alpha$ unbounded in $\alpha \rightarrow A_\alpha \cap B_n^\alpha \neq \emptyset]$. Set $\mathcal{G} = \langle G, E \rangle$, where $G \stackrel{\text{def}}{=} \kappa$ and $\{\nu, \alpha\} \in E \leftrightarrow \alpha \in S \ \& \ \nu \in A_\alpha$ for all $\nu < \alpha < \kappa$.

We first show that $\text{ch}(\mathcal{G}) \geq \omega_1$. Let $f : \kappa \rightarrow \omega$. Set $B_n = f^{-1}\{n\}$ for each n . Let α_0 exceed $\sup(B_n)$ for all those n with $\sup(B_n) < \kappa$. Let

$$C = \{\alpha \in \kappa \mid \alpha > \alpha_0 \ \& \ \forall n [B_n \text{ unbounded in } \kappa \rightarrow B_n \cap \alpha \text{ unbounded in } \alpha]\}.$$

C is clearly closed and unbounded in κ , so we can pick $\alpha \in C$, $\text{cf}(\alpha) = \omega$, so that $\forall n \in \omega (B_n \cap \alpha = B_n^\alpha)$. Since $\alpha \in C$, $\alpha > \alpha_0$, so $f(\alpha) \in B_n$ for some n with $\sup(B_n) = \kappa$. Thus B_n^α is unbounded in α . Thus $A_\alpha \cap B_n^\alpha \neq \emptyset$. Pick $\nu \in A_\alpha \cap B_n^\alpha$. Then $f(\nu) = n$ and $\{\nu, \alpha\} \in E$. Hence f is not a colouring of $\mathcal{G}$.

We show next that $\text{ch}(\mathcal{G} \upharpoonright \lambda) \leq \omega$ for all $\lambda < \kappa$. It suffices to show that there is an enumeration $\langle x_\nu \mid \nu < \theta \rangle$ of λ such that $\{\eta < \nu \mid \{x_\eta, x_\nu\} \in E\}$ is finite for all $\nu < \theta$. (We can then colour $\mathcal{G} \upharpoonright \lambda$ by a simple induction along this ordering, using only countably many colours.) We prove this by induction on λ . For $\lambda = 0$ there is nothing to prove. For successor λ the induction step is trivial. Suppose then that $\text{lim}(\lambda)$. Let $\gamma = \text{cf}(\lambda)$. Let $C \subseteq \lambda$ be closed and unbounded in λ , $\text{otp}(C) = \gamma$, $C \cap S = \emptyset$. Let $\langle \alpha_\nu \mid \nu < \gamma \rangle$ be the canonical enumeration of C . For each $\nu < \gamma$, let $<_\nu$ be a suitable ordering (i.e. enumeration of $\mathcal{G} \upharpoonright (\alpha_{\nu+1} - \alpha_\nu)$). Define an ordering (i.e. enumeration) $<_\lambda$ of $\mathcal{G} \upharpoonright \lambda$ by: $x <_\lambda y \leftrightarrow \exists \nu < \gamma [x <_\nu y \text{ or } x < \alpha_\nu \leq y]$. This ordering of $\mathcal{G} \upharpoonright \lambda$ is as required. For suppose $y < \lambda$. Pick ν with $\alpha_\nu \leq y < \alpha_{\nu+1}$. Suppose $x <_\lambda y$ and $\{x, y\} \in E$. If $x < \alpha_\nu$, then we must have $y \in S$ and $x \in A_\nu$, so $y > \alpha_\nu$ and x lies in the finite set $A_\nu \cap \alpha_\nu$. On the other hand, if $\alpha_\nu \leq x$, then $x <_\nu y$, so x lies in the finite set $\{x <_\nu y \mid \{x, y\} \in E\}$. The proof is complete. $\square$

15. Other results

In this section we summarise, very briefly, one or two further results on constructibility. Firstly, what effect does the assumption $V = L$ have upon model theory. Since GCH has a strong influence in this area, one might expect that $V = L$ has an even stronger effect. This is indeed the case. Of the many results known to date, the most striking concerns the so-called “gap” theorems. Here, one takes some fixed, countable, first-order language S , containing a distinguished unary predicate U , and denotes by $\langle \kappa, \lambda \rangle \rightarrow \langle \kappa', \lambda' \rangle$ the following “Löwenheim–Skolem Theorem”: Every S -structure $\mathfrak{A}$ with $|\mathfrak{A}| = \kappa$ and $|U^\mathfrak{A}| = \lambda$ is elementarily equivalent to a structure $\mathfrak{B}$ with $|\mathfrak{B}| = \kappa'$ and $|U^\mathfrak{B}| = \lambda'$. An old result of Vaught says that if $\beta \geq \omega$, then $\langle \omega_{\alpha+\beta}, \omega_\alpha \rangle \rightarrow \langle \omega_\gamma, \omega_\delta \rangle$ for all γ, δ , assuming GCH. And by simple examples, it is easily shown that if $\delta > \beta$ ($\beta < \omega$), then $\langle \omega_{\alpha+\beta}, \omega_\alpha \rangle \not\rightarrow \langle \omega_{\gamma+\delta}, \omega_\gamma \rangle$. Since $\langle \omega_{\alpha+\beta}, \omega_\alpha \rangle \rightarrow \langle \omega_{\alpha+\delta}, \omega_\alpha \rangle$ is just a special case of the usual, downward Löwenheim–Skolem Theorem, if $\delta < \beta$, it follows that the only interesting cases left are those of the form $\langle \omega_{\alpha+n}, \omega_\alpha \rangle \rightarrow \langle \omega_{\beta+n}, \omega_\beta \rangle$. Assuming GCH, the only positive result known to date is Chang’s Theorem, that $\langle \omega_{\alpha+1}, \omega_\alpha \rangle \rightarrow \langle \omega_{\beta+1}, \omega_\beta \rangle$ for ω_β regular. Assuming $V = L$, however, the problem has a complete solution.

15.1. THEOREM (Jensen). *Assume $V = L$. Then for all β and all n , $\langle \omega_{\alpha+n}, \omega_\alpha \rangle \rightarrow \langle \omega_{\beta+n}, \omega_\beta \rangle$.*

The proof of “Chang’s Theorem” for the singular cardinal case only requires the combinatorial principle $\square$. But all other cases of the above require extremely heavy fine-structure machinery (morasses). Some idea of this machinery is provided in DEVLIN [1973], where the easiest case is dealt with.

Further results are also possible in the theory of trees in L . A κ -Kurepa tree is a κ -tree with at least κ^+ κ -branches. It is known from work of Silver that the existence of such trees is unprovable in ZFC, even with GCH. (See Theorem 5.7 of Chapter B.4.) In L , however, they are quite common. Specifically, we have:

15.2. THEOREM (Jensen). *Assume $V = L$. Let κ be an uncountable regular cardinal. Then there is a κ -Kurepa tree iff κ is not ineffable.*

(A cardinal κ is *ineffable* if, whenever $f : [\kappa]^2 \rightarrow 2$, there is a stationary set which is homogeneous for f . Thus ineffability is a generalisation of weak compactness. It is, however, much stronger than weak compactness.)

The assumption $V = L$ also has a strong effect upon the descriptive set theory of the continuum. This is mainly due to the following result of Gödel:

15.3. THEOREM (Gödel). *Assume $V = L$. Then there is a Δ_2^1 well-ordering of $\mathcal{P}(\omega)$ of type ω_1 .*

Details of all of the above results are given in DEVLIN [1973].

Some of the more recent developments in constructibility theory have concerned not the “inside” of L , but the relationship between L and V . The limitations of space do not allow us to elaborate, but it seems that there is no possibility of adopting a compromising approach to “ $V = L$ ”. Either V is “very much like” L , or else “very unlike” L . We expect to include details of the relevant results (due to Jensen) in the forthcoming revised edition of DEVLIN [1973].

Historical Note

The material covered in Sections 1 and 2 is due to Gödel. The results of Sections 3–7 were undoubtedly known to Gödel, though some of them perhaps only “implicitly”. The first explicit reference to the fact that the constructible hierarchy and its canonical well-ordering are Σ_1^{ZF} occurs in

work of Jensen and Karp, who used primitive recursive functions to obtain this result. The proofs given here are our own versions, though we make no claims as to originality.

From Section 8 onwards, with only minor exceptions, everything covered is due to Jensen.

References

DEVLIN, K.J.

[1973] *Aspects of Constructibility*, Lecture Notes in Mathematics, Vol. 354 (Springer, Berlin).

DEVLIN, K.J. and H. JOHNSBRÄTEN

[1974] *The Souslin Problem*, Lecture Notes in Mathematics, Vol. 405 (Springer, Berlin).

GÖDEL, K.

[1938] *The Consistency of the Axiom of Choice and of the Generalised Continuum-Hypothesis*, Annals of Mathematics Studies, Vol. 3 (Princeton Univ. Press, Princeton, NJ).

B.6

Martin's Axiom

MARY ELLEN RUDIN

Martin's axiom, known as MA, can be stated in a number of different ways. The topological form of MA is easy to remember. The Boolean algebra form is sometimes reassuringly familiar. But the partial order form is the useful one. It is an unfamiliar hurdle for nonlogicians. But it is more or less necessary for efficient use of MA; it is a first step in forcing techniques; and it is really not difficult.

If $\langle P, \geq \rangle$ is a partially ordered set, then $D \subset P$ is *dense* provided, for each $p \in P$, there is a $d \in D$ with $p \geq d$. A subset Q of P is *compatible* provided, for each finite subset F of Q , there is a $q \in P$ such that $p \geq q$ for all $p \in F$. ccc is read *countable chain condition* and $\langle P, \geq \rangle$ is ccc provided every pairwise incompatible subset is countable.

MARTIN'S AXIOM: *Suppose that $\langle P, \geq \rangle$ is a ccc partially ordered set and $\mathcal{D}$ is a family of less than 2^ω dense subsets of P . Then there is a compatible subset Q of P which meets every member of $\mathcal{D}$.*

In Section 6 of Chapter B.4 Burgess proves:

1. THEOREM. *If ZFC is consistent, then $\text{ZFC} + \text{MA} + \neg \text{CH}$ is consistent.*

MA is also known to be independent of $\neg \text{CH}$.

We begin by proving that the above partial order form of MA implies the topological form; actually they are equivalent.

A topological space is ccc if every family of disjoint open sets is countable.

2. THEOREM (MA)*. *If X is a ccc compact Hausdorff space, then X is not the union of less than 2^ω nowhere dense sets.*

PROOF. Suppose that $\omega \leq \lambda < 2^\omega$, that X is a ccc compact Hausdorff space, and that $\{X_\alpha\}_{\alpha \in \lambda}$ is a family of nowhere dense subsets of X .

Let P be the set of all nonempty open sets in X and partially order P by $p \leq q$ if $p \subset q$. Since X is ccc so is P . For $\alpha \in \lambda$, define $D_\alpha = \{p \in P \mid \bar{p} \cap X_\alpha = \emptyset\}$; each D_α is dense in P . Hence there is a compatible $Q \subset P$ which intersects every D_α . Q is a basis for a filter and X is compact, so there is an $x \in \bigcap \{\bar{q} \mid q \in Q\}$. For each $\alpha \in \lambda$ there is a $q \in Q$ with $\bar{q} \cap X_\alpha = \emptyset$, so $x \notin X_\alpha$. Hence $X \neq \bigcup_{\alpha \in \lambda} X_\alpha$. $\square$

If CH, then Theorem 2 is just the Baire category theorem, so as no surprise:

* We write "Theorem (MA)" to indicate that we use Martin's Axiom to prove the theorem.

3. THEOREM. CH implies MA.

PROOF. Suppose that $\{D_n\}_{n \in \omega}$ is a family of dense subsets of a ccc partially ordered set $\langle P, \geq \rangle$. By induction choose $d_n \in D_n$ such that $d_n > d_{n+1}$ for all n . Then $\{d_n\}_{n \in \omega}$ is a compatible subset of P which meets every D_n . $\square$

A basic fact about partial orders is:

4. THEOREM (MA + $\neg$ CH). If $\langle P, \geq \rangle$ is a ccc partial order and $R \subset P$ is uncountable, then there is an uncountable compatible $Q \subset R$.

PROOF. Without loss of generality $|R| = \omega_1$. Let

$$G = \{p \in P \mid |\{q \in R \mid p \text{ and } q \text{ are compatible}\}| = \omega\}.$$

Let G^* be a maximal pairwise incompatible subset of G . Let $P^* = \{p \in P \mid p \text{ is not compatible with any } q \in G^*\}$ and let $R^* = R \cap P^*$.

Since $\langle P, \geq \rangle$ is ccc, G^* is countable and $R - R^*$ is countable. Thus there is a one-to-one indexing $\{q_\alpha\}_{\alpha \in \omega_1}$ of R^* .

Let P' be the set of all finite, compatible in $\langle P, \geq \rangle$, subsets of P^* . Observe that if $F \in P'$ and $p \geq q$ for all $p \in F$, then $q \in P^*$. Thus P' , partially ordered by reverse inclusion is ccc.

For each $\alpha \in \omega_1$, define $D_\alpha = \{F \in P' \mid F \cap \{q_\beta\}_{\beta > \alpha} \neq \emptyset\}$.

For each $F \in P'$ there is a $q \in P^*$ with $p \geq q$ for all $p \in F$. Since q is compatible with uncountably many q_β , each D_α is dense in P' . So there is a compatible $Q' \subset P'$ which meets every D_α . Thus $Q = \bigcup Q'$ is an uncountable compatible subset of P . $\square$

Recall (see Chapter B.3) that a Souslin tree is an uncountable tree with no uncountable chains or antichains. In a tree a compatible set in reverse order is a chain; so Theorem 4 yields:

5. THEOREM (MA + $\neg$ CH). There is no Souslin tree.

A Souslin tree can be used to build a Souslin line — a connected, linearly ordered, ccc space which is not separable. It is well known that the product of two Souslin lines is *not* ccc. However:

6. THEOREM (MA + $\neg$ CH). The product of any family of ccc spaces is ccc.

PROOF. By a simple Δ -system argument (not using MA, see Theorem 5.8 of

Chapter B.3), if a product is not ccc, then some subproduct of finitely many factors is not ccc. So to prove Theorem 6 we need only show that the product of any two ccc spaces is ccc.

Suppose that X and Y are ccc and that $\{U_\alpha \times V_\alpha\}_{\alpha \in \omega_1}$ are disjoint, nonempty basic open sets in $X \times Y$. Let P be the set of all nonempty open sets in X partially ordered by inclusion. By Theorem 4 there is an uncountable compatible subset Q of $\{U_\alpha\}_{\alpha \in \omega_1}$. But if U_α and U_β belong to Q , $U_\alpha \cap U_\beta \neq \emptyset$ so $V_\alpha \cap V_\beta = \emptyset$. Thus $\{V_\alpha \mid U_\alpha \in Q\}$ is a family of disjoint open sets which contradicts the fact that Y is ccc. $\square$

MA was first discovered by MARTIN and SOLOVAY [1970], who observed that MA was inherent in a number of previous proofs of the consistency that there be no Souslin trees. Their original paper is a beautiful explanation of MA which I recommend. They stress the usefulness of MA as a viable alternative to CH. They point out that many of the traditional problems solved using CH can be solved using MA alone. Frequently the part of CH that is used is only MA. But almost equally often, a statement *true* under CH can be proved *false* under $MA + \neg CH$. Since $MA + \neg CH$ is consistent with ZFC, any such statement is itself independent of ZFC.

MA is severely limited by the fact that it only says something interesting about cardinals λ where $\omega < \lambda < 2^\omega$. However these are precisely the cardinals which most often cause grief for nonlogicians. Certainly general topologists have found MA applicable to a rich variety of their problems. Those discussed by Juhász in Chapter B.7 give some feeling for its use and we will not attempt to give references for the multitude of other topological uses of MA.

An analyst who works with Banach spaces recently asked me two questions. Must a compact Hausdorff space of cardinality $\leq 2^\omega$ be sequentially compact? Must a ccc compact Hausdorff space with a point countable separating family of open F_σ 's be metrizable? Neither question can be answered in ZFC. The analyst already knew that $MA + \neg CH$ implies that the answer to both questions is yes. Analysts too are beginning to use and recognize MA.

An important recent result using MA is in algebra. Shelah has recently proved that Whitehead's problem is undecidable in ZFC: if $V = L$, then every W -group is free; but if $MA + \neg CH$, there is a W -group which is not free. There is an excellent description of Whitehead's problem and Shelah's solution written for the Monthly by EKLOF [1977] so we will avoid the necessary definitions and heartily recommend the reading of Eklof's article.

Another recommended Monthly article, written by SHOENFIELD [1975], gives an elegant, elementary discussion of MA and proves many of the same theorems given here.

Shelah's solution of Whitehead's problem illustrates the relationship between $MA + \neg CH$ and $V = L$ often seen in topology. Roughly speaking, $MA + \neg CH$ completely unravels the area between $\omega = 2^\omega$ while $V = L$ holds it completely rigid. Anyway these two axioms are strongly contrasting and often yield contradictory theorems.

Let us turn now to some of the combinatorial consequences of MA:

7. THEOREM (MA). *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are families of cardinality less than 2^ω of subsets of ω such that, for all finite subsets $\mathcal{C}$ of $\mathcal{A}$ and elements B of $\mathcal{B}$, $B - \bigcup \mathcal{C}$ is infinite. Then there is an $M \subset \omega$ such that $B - M$ is infinite for all $B \in \mathcal{B}$ but $A - M$ is finite for all $A \in \mathcal{A}$.*

PROOF. Index $\mathcal{A} = \{A_\alpha\}_{\alpha \in \lambda}$ and $\mathcal{B} = \{B_\alpha\}_{\alpha \in \lambda}$ for some $\lambda < 2^\omega$. Let $P = \{\langle H, K \rangle \mid H \text{ is a finite subset of } \lambda \text{ and } K \text{ is a finite subset of } \omega\}$. Define $\langle H, K \rangle \geq \langle H', K' \rangle$ in P provided $H \subset H'$, $K \subset K'$, and $(K' - K) \cap \bigcup_{\alpha \in H} A_\alpha = \emptyset$.

Any uncountable subset of P has two members with the same second element, say $\langle H, K \rangle$ and $\langle H', K \rangle$. Since $\langle H, K \rangle \geq \langle (H \cup H'), K \rangle$ and $\langle H', K \rangle \geq \langle (H \cup H'), K \rangle$, P is ccc.

For each $\alpha \in \lambda$, define $D_\alpha = \{\langle H, K \rangle \in P \mid \alpha \in H\}$. For $\alpha \in \lambda$ and $n \in \omega$, define $E_{\alpha, n} = \{\langle H, K \rangle \in P \mid |K \cap B_\alpha| > n\}$. It is easy to check that each member of $\mathcal{D} = \{D_\alpha \mid \alpha \in \lambda\} \cup \{E_{\alpha, n} \mid \alpha \in \lambda \text{ and } n \in \omega\}$ is dense in P . Since $|\mathcal{D}| = \lambda < 2^\omega$, MA implies that there is a compatible subset Q of P which meets every member of $\mathcal{D}$.

Define $M = \omega - \bigcup \{K \mid \langle H, K \rangle \in Q\}$. If $\alpha \in \lambda$ there is $\langle H, K \rangle \in Q \cap D_\alpha$. If $\langle H', K' \rangle$ is any other member of Q , since Q is compatible, there is $\langle H'', K'' \rangle \in Q$ such that $\langle H'', K'' \rangle \leq \langle H, K \rangle$ and $\langle H'', K'' \rangle \leq \langle H', K' \rangle$. Since $K' \subset K''$ and $(K'' - K') \subset A_\alpha$, $(K' - A_\alpha) \subset K$. Thus $A_\alpha - M \subset K$ so $A_\alpha - M$ is finite.

Since for each $n \in \omega$ there is an $\langle H, K \rangle \in Q$ with $|K \cap B_\alpha| > n$, $B_\alpha - M$ is infinite for all $\alpha \in \lambda$. $\square$

The proof of Theorem 7 is typical of MA proofs. With $\lambda = \omega$, this theorem is a frequently used fact which does not need MA in its proof. But MA allows us to extend the theorem to all cardinals less than 2^ω although such an extension would be false without some set theoretic assumption beyond ZFC.

Two direct consequences of Theorem 7 which are sometimes more immediately applicable are:

8. COROLLARY (MA). *If $\mathcal{B}$ is a family of cardinality less than 2^ω of subsets of ω with each finite subset of $\mathcal{B}$ having infinite intersection, then there is an infinite subset L of ω such that $L - B$ is finite for all $B \in \mathcal{B}$.*

PROOF. Define $\mathcal{A}^* = \{(\omega - B) \mid B \in \mathcal{B}\}$ and $B^* = \{\omega\}$. By Theorem 7 applied to $\mathcal{A}^*$, $\mathcal{B}^*$, there is an M such that $A - M$ is finite for all $A \in \mathcal{A}^*$ but $\omega - M$ is infinite. Define $L = \omega - M$. $\square$

9. COROLLARY (MA). *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are families of cardinality less than 2^ω of subsets of ω such that $B - \bigcup \mathcal{C}$ is infinite for all $B \in \mathcal{B}$ and finite $\mathcal{C} \subset \mathcal{B}$. Then, if $|\mathcal{A} \cup \mathcal{B}| = \lambda$, there is an infinite subset L of ω such that $A \cap L$ is finite for all $A \in \mathcal{A}$ and $B \cap L$ is infinite for all $B \in \mathcal{B}$.*

PROOF. By Theorem 7 there is an $M \subset \omega$ such that $A - M$ is finite for all $A \in \mathcal{A}$ and $B - M$ is infinite for all $B \in \mathcal{B}$. Define $L = \omega - M$. Then, for $B \in \mathcal{B}$, $B - M = B - (\omega - L) = L - (\omega - B) = L \cap B$ is infinite. Similarly $L \cap A$ is finite for all $A \in \mathcal{A}$. $\square$

A consequence of Corollary 8 is:

10. COROLLARY (MA). *If $\lambda < 2^\omega$, then 2^λ is sequentially compact.*

PROOF. Let $\{f_n\}_{n \in \omega}$ be an infinite subset of 2^λ . We show that, if f is an arbitrary limit point of $\{f_n\}_{n \in \omega}$, then there is an $L \subset \omega$ such that $\{f_n\}_{n \in L}$ converges to f .

Let G be the set of all functions into 2 which f extends whose domain is a finite subset of λ . For $g \in G$ let $B_g = \{n \in \omega \mid f_n \text{ extends } g\}$. Since $|G| = \lambda$, the hypotheses of Corollary 8 are satisfied and there is an infinite $L \subset \omega$ such that $L - B_g$ is finite for all $g \in G$. L clearly has the desired property. $\square$

Actually, in Corollary 10, 2^λ may be replaced by any compact Hausdorff space of cardinality less than 2^{2^ω} (see Corollary 1 to Theorem 1.7 in Chapter B.7).

For an application of Corollary 9, define $F = \{f : \omega \rightarrow \omega\}$ with $f < g$ in F provided there is an $n \in \omega$ with $f(k) < g(k)$ for all $k > n$. A subset G of F is *dominating* provided, for every $f \in F$ there is a $g \in G$ with $g > f$.

$\{f_\alpha\}_{\alpha < \lambda} \subset F$ is called a *scale* if it is dominating and $\alpha < \beta < \lambda$ implies that $f_\alpha < f_\beta$.

11. COROLLARY (MA). *Every dominating family has cardinality 2^ω , and there is a scale.*

PROOF. Suppose that $\lambda < 2^\omega$ and that $\{f_\alpha\}_{\alpha \in \lambda} \subset F$. For $\alpha \in \lambda$, define $A_\alpha = \{\langle i, j \rangle \in \omega^2 \mid j \leq f(i)\}$ and for $i \in \omega$ define $B_i = \{i\} \times \omega$. By Corollary 9 there is an $L \subset \omega^2$ such that all $A_\alpha \cap L$ are finite and $B_i \cap L$ are infinite. Choose $f \in F$ with $(i, f(i)) \in L$ for all $i \in \omega$. Then $f_\alpha < f$ for all $\alpha \in \lambda$. $\square$

A trivial consequence of Corollary 11 is that 2^ω is regular. A consequence of Corollary 9 (which was first used to show the consistency of a counterexample to the normal Moore space conjecture) is the following.

12. THEOREM (MA). *If X is a subset of the real numbers of cardinality less than 2^ω , then every subset of X is a relative G_δ set.*

PROOF. Suppose that $Y \subset X$ and that $\{U_n\}_{n \in \omega}$ is a countable open basis for the real numbers such that no pair of distinct numbers is in the intersection of infinitely many U_n 's.

Index $Y = \{y_\alpha\}_{\alpha \in \lambda}$ and $X - Y = \{x_\alpha\}_{\alpha \in \lambda}$: we assume without loss of generality that neither is empty and repetitions do not matter. For $\alpha \in \lambda$, let $B_\alpha = \{n \in \omega \mid y_\alpha \in U_n\}$ and let $A_\alpha = \{n \in \omega \mid x_\alpha \in U_n\}$. Define $\mathcal{A} = \{A_\alpha\}_{\alpha \in \lambda}$ and $\mathcal{B} = \{B_\alpha\}_{\alpha \in \lambda}$. By Corollary 10 there is an $L \subset \omega$ such that $L \cap B_\alpha$ is infinite and $L \cap A_\alpha$ is finite for all $\alpha \in \lambda$. For $n \in \omega$ define $L_n = \bigcup_{m \in M} U_m$. Since each $B_\alpha \cap L$ is infinite, $y_\alpha \in \bigcap_{n \in \omega} L_n$. But each $A_\alpha \cap L$ is finite so $x_\alpha \notin \bigcap_{n \in \omega} L_n$. Thus Y is a relative G_δ . $\square$

If X is infinite, the cardinality of the set of all G_δ sets in X is 2^ω , and the cardinality of all subsets of X is 2^λ . Thus Theorem 12 yields:

13. COROLLARY (MA). *If $\omega \leq \lambda < 2^\omega$, then $2^\omega = 2^\lambda$.*

Another Baire category type theorem is:

14. THEOREM (MA). *Suppose that $0 < \lambda < 2^\omega$, that X is a space with a countable basis, and that $\{X_\alpha\}_{\alpha \in \lambda}$ is a family of nowhere dense subsets of X . Then $\bigcup_{\alpha \in \lambda} X_\alpha$ is the union of countably many nowhere dense sets.*

PROOF. Let $\{U_n\}_{n \in \omega}$ be a basis for the topology of X : make sure that each basis element is indexed with infinitely many different n . Then define $B_n = \{m \in \omega \mid U_m \subset U_n\}$. For each $\alpha \in \lambda$ define $A_\alpha = \{n \in \omega \mid U_n \cap X_\alpha \neq \emptyset\}$. Let $\mathcal{B} = \{B_n \mid n \in \omega\}$ and $\mathcal{A} = \{A_\alpha \mid \alpha \in \lambda\}$. By Corollary 9 there is an $L \subset \omega$ such that $L \cap B_n$ is infinite for all $n \in \omega$ but $L \cap A_\alpha$ is finite for all $\alpha \in \lambda$. Thus if $Y_n = X - \bigcup \{m \in L \mid m > n\}$, Y_n is nowhere dense and, for each $\alpha \in \lambda$, there is an n with $X_\alpha \subset Y_n$. Therefore $\bigcup_{\alpha \in \lambda} X_\alpha$ is the union of countably many nowhere dense sets. $\square$

REMARK. All the consequences 7–14 of MA were in fact proved from 7. Actually, van Douwen has shown that the simpler 8 implies 7 (and hence 7–14). To see this, let $\mathcal{A}, \mathcal{B}$ be as in 7, and let

$$\mathcal{D} = \{[\omega - n]^{<\omega} \mid n \in \omega\} \cup \{[s \in [\omega]^{<\omega} \mid s \cap B \neq \emptyset] \mid B \in \mathcal{B}\} \\ \cup \{[\omega - A]^{<\omega} \mid A \in \mathcal{A}\}$$

(where $[I]^{<\omega}$ is the set of all finite subsets of I). Apply 8 to $\mathcal{D}$ to get an $L \subset [\omega]^{<\omega}$ with $L - X$ finite for all $X \in \mathcal{D}$, and let $M = \omega - \bigcup L$. It is known that 4–6 and 15–17 do not follow from 8.

Baire category theorems, Borel hierarchy, and measure theory type theorems go together. One consequence of the following theorem is that the union of any family of less than 2^ω measurable sets of real numbers is measurable. We use R for the real line and $m(X)$ for the Lebesgue measure of X .

15. THEOREM (MA). *If $0 \leq \lambda < 2^\omega$ and for each $\alpha \in \lambda$, $X_\alpha \subset R$ and $m(X_\alpha) = 0$, then $m(\bigcup_{\alpha \in \lambda} X_\alpha) = 0$.*

PROOF. Suppose that $\varepsilon < 0$. We prove Theorem 15 by showing that there is an open subset Y of R such that $m(Y) \leq \varepsilon$ and $X_\alpha \subset Y$ for all $\alpha \in \lambda$.

Define $P = \{U \subset R \mid U \text{ is open and } m(U) < \varepsilon\}$ and partially order P by reverse inclusion.

Define $\mathcal{B}$ to be a countable family of open intervals which form a basis for R . Let $\mathcal{B}^*$ be the set of all finite unions of members of $\mathcal{B}$.

If S is an uncountable subset of P , there is an uncountable subset S' of S and a $0 < n \in \omega$ such that $U \in S'$ implies that $m(S) + 1/n < \varepsilon$. For each $U \in S'$ choose $U^* \subset U$ such that $U^* \in \mathcal{B}^*$ and $m(U - U^*) < 1/n$. Since S' is uncountable and $\mathcal{B}^*$ is countable, there must be different terms U and V

of S' with $U^* = V^*$. Then U and V are compatible since $m(U \cup V) < \varepsilon$; thus $\langle P, \subset \rangle$ is ccc.

For each $\alpha \in \lambda$ define $D_\alpha = \{U \in P \mid X_\alpha \subset U\}$. Since D_α is dense there is a compatible $Q \subset P$ which meets every D_α . Let $Y = \bigcup Q$. For all $\alpha \in \lambda$, $X_\alpha \subset Q$. Since R is hereditarily Lindelöf, countably many members of Q cover Y so, if $m(Y) > \varepsilon$, there is some finite subset Q' of Q with $m(\bigcup Q') > \varepsilon$. However, since Q is compatible, there is a $Y' \in P$ with $\bigcup Q' \subset Y'$. Since $m(Y') < \varepsilon$ we have a contradiction. Thus $m(Y) \leq \varepsilon$ and Y has all of the desired properties. $\square$

An Aronszajn tree is a tree $\langle T, \leq \rangle$ of cardinality ω_1 having no uncountable level or chain. A Souslin tree is an Aronszajn tree in which every antichain is countable (see Chapter B.3). $\text{MA} + \neg \text{CH}$ denies the existence of a Souslin tree in an especially strong way:

16. THEOREM (Baumgartner; $\text{MA} + \neg \text{CH}$). *Every Aronszajn tree is the union of countably many antichains.*

(Such an Aronszajn tree is called *special*.)

PROOF. Let $\langle T, \leq \rangle$ be an Aronszajn tree. Our aim is to define a function $q : T \rightarrow \mathbb{Q}$ (where $\mathbb{Q}$ is the set of all rational numbers) such that $s < t$ in T implies that $q(s) < q(t)$. Since $q^{-1}(r)$ for each $r \in \mathbb{Q}$ will then be an antichain, Theorem 16 will then be proved.

Let $P = \{f : S \rightarrow \mathbb{Q} \mid S \text{ is a finite subset of } T \text{ and } s < t \text{ in } S \text{ implies that } f(s) < f(t)\}$. Define $f \geq g$ in P provided g extends f . For each $t \in T$ define $D_t = \{f \in P \mid t \in \text{domain of } f\}$. Each D_t is dense in P and $|T| = \omega_1$ so, if P is ccc, there is a compatible $P' \subset P$ which meets every D_t . Thus there is a $q : T \rightarrow \mathbb{Q}$ which extends every $f \in P'$, and this q has the desired properties.

It remains to prove that P is ccc. Assume that $\{f_\alpha\}_{\alpha \in \omega_1} \subset P$ and that the domain of f_α is S_α . We prove that P is ccc by showing that there are $\alpha < \beta$ in ω_1 and $f \in P$ such that f extends both f_α and f_β .

By a Δ -system argument (see Chapter B.3) we can choose an $n \in \omega$, a $k \in \omega$, and an infinite (uncountable) subset M of ω_1 such that:

(a) For all $\alpha \in M$, S_α has n terms $s_{0\alpha}, s_{1\alpha}, \dots, s_{n-1,\alpha}$.

(b) $\alpha \neq \beta$ in M and $i \in n$ imply $f_\alpha(s_{i\alpha}) = f_\beta(s_{i\beta})$.

(c) $\alpha \neq \beta$ in M and $i \in k$ imply $s_{i\alpha} = s_{i\beta}$.

(d) $\alpha < \beta$ in M and i and j in $n - k$ imply that the level in T to which $s_{i\alpha}$ belongs precedes the level in T to which $s_{j\beta}$ belongs.

(e) $i \in n - k$ implies that $\{s_{i\alpha}\}_{\alpha \in M}$ is an antichain.

To see that you can get (e), recall that if M' is any uncountable subset of ω_1 , then $\{s_{i\alpha}\}_{\alpha \in M'}$ must contain an uncountable antichain since otherwise M' (with the induced order) would be a Souslin tree which is denied by $\text{MA} + \neg \text{CH}$.

Suppose that (i, j) is a pair of numbers in $n - k$. We now use Ramsey's theorem: $\omega \rightarrow (\omega)_2^2$ (see Chapter B.3). Let $A = \{\text{pairs } (\alpha, \beta) \text{ of terms of } M \mid \alpha < \beta \text{ and } s_{\alpha i} < s_{\beta j}\}$ and let $B = \{\text{pairs } (\alpha, \beta) \text{ of terms of } M \mid \alpha < \beta \text{ and } s_{\alpha i} \not< s_{\beta j}\}$. There can be no $\alpha < \beta < \gamma$ all of whose pairs are in A since then $s_{\alpha i} < s_{\gamma j}$ and $s_{\beta i} < s_{\gamma j}$ which by (d) would mean that $s_{\alpha i} < s_{\beta i}$ would contradict (e). So there is an infinite $M' \subset M$ all of whose pairs are in B .

For different i and j in $n - k$ choose successively smaller infinite M' 's until we have an infinite $M^* \subset M$ such that for all $\alpha < \beta$ in M^* and i and j in $n - k$, $s_{\alpha i} \not< s_{\beta j}$. Then, for $\alpha < \beta$ in M^* , $f: (S_\alpha \cup S_\beta) \rightarrow \mathbb{Q}$ defined by $f(s) = f_\alpha(s)$ for $s \in S_\alpha$, and $f_\beta(s)$ for $s \in S_\beta$ is well defined and belongs to P and extends both f_α and f_β . $\square$

A similar proof (with a different proof that P is ccc) would show that under $\text{MA} + \neg \text{CH}$, every Aronszajn tree $\langle T, \leq \rangle$ is normal (under the topology induced by taking all sets of the form $\{x \in T \mid s < x \leq t\}$ where $s < t$ in T as a basis).

We close with a combinatorial theorem. A family $\mathcal{A}$ of sets is called *almost disjoint* if the intersection of each pair of distinct elements of $\mathcal{A}$ is finite.

17. THEOREM (Wage; MA). *Suppose that κ is regular and $\omega < \kappa \leq \lambda < 2^\omega$. If $\mathcal{A}$ is a family of λ almost disjoint countable subsets of κ , then there is a $B \subset \kappa$ of cardinality κ such that $\mathcal{A} \cup \{B\}$ is almost disjoint.*

PROOF. Let $\mathcal{A} = \{A_\alpha\}_{\alpha \in \lambda}$. Define $P = \{\langle H, K \rangle \mid H \text{ is a finite subset of } \mathcal{A} \text{ and } K \text{ is a finite subset of } \kappa\}$. Partially order P by $\langle H, K \rangle \geq \langle H', K' \rangle$ in P provided $H \subset H'$, $K \subset K'$, and $(K' - K) \cap (\bigcup H) = \emptyset$.

Let $\{\langle H_\alpha, K_\alpha \rangle\}_{\alpha \in \omega_1}$ be an uncountable subset of P . By a Δ -system argument (see Chapter B.3), there is an uncountable $M \subset \omega_1$, $n \in \omega$, $H \subset \lambda$, and $K \subset \kappa$ such that $\alpha \neq \beta$ in M implies that $H_\alpha \cap H_\beta = H$ and $K_\alpha \cap K_\beta = K$, and $\alpha \in M$ implies that $K_\alpha - K$ has n terms. Observe that $\{K_\alpha - K\}_{\alpha \in M}$ are disjoint and $\{\bigcup (H_\alpha - H)\}_{\alpha \in M}$ are almost disjoint. Let C be any infinite countable subset of M . Since each $\bigcup_{\alpha \in C} H_\alpha$ is countable and $\{K_\alpha - K\}_{\alpha \in M}$ are disjoint, we can choose an $L \subset M$ such that $|L| > n$ and $(\bigcup_{\alpha \in C} H_\alpha) \cap (\bigcup_{\beta \in L} K_\beta - K) = \emptyset$. Since $|L| > n$, $|K_\alpha - K| = n$ for all

$\alpha \in C$, and $\{\bigcup (H_\beta - H)\}_{\beta \in L}$ are almost disjoint, there is an $\alpha \in C$ and $\beta \in L$ such that $(K_\alpha - K) \cap (\bigcup (H_\beta - H)) = \emptyset$. Hence $\langle H_\alpha, K_\alpha \rangle \geq \langle (H_\alpha \cup H_\beta), (K_\alpha \cup K_\beta) \rangle$ and $\langle H_\beta, K_\beta \rangle \geq \langle (H_\alpha \cup H_\beta), (K_\alpha \cup K_\beta) \rangle$. Thus P is ccc.

For $\alpha \in \lambda$, let $X_\alpha = \{\langle H, K \rangle \in P \mid \alpha \in H\}$ and, for $\beta \in \kappa$ let $Y_\beta = \{\langle H, K \rangle \in P \mid (\kappa - B) \cap K \neq \emptyset\}$. Since both X_α and Y_β are dense in P for all $\alpha \in \lambda$ and $\beta \in \kappa$, there is a compatible Q which meets every X_α and Y_β . Let $B = \bigcup \{K \subset \kappa \mid \langle H, K \rangle \in Q\}$. Since $Q \cap Y_\beta \neq \emptyset$ for all $\beta \in \kappa$, $|B| = \kappa$. If $\alpha \in \lambda$, there is an $\langle H, K \rangle \in Q \cap X_\alpha$. If $\langle H', K' \rangle$ is any other member of Q , there is $\langle H'', K'' \rangle \in P$ with $\langle H, K \rangle \geq \langle H'', K'' \rangle$ and $\langle H', K' \rangle \geq \langle H'', K'' \rangle$. Since $(K'' - K) \cap A_\alpha = \emptyset$ and $K' \subset K''$, $K' \cap A_\alpha \subset K$. Thus $B \cap A_\alpha \subset K$ so $B \cap A_\alpha$ is finite. $\square$

From this mixed bag of theorems can we generalize about *when* we should expect MA to be useful? In topology $\text{MA} + \neg \text{CH}$ can be used to construct a variety of normal but not collectionwise normal spaces. MA can be used to deny the existence of certain pathologies in ccc spaces. MA often has something to say about problems involving compact Hausdorff spaces. For instance many of the traditional theorems about $\beta\mathbb{N}$ (the Stone-Čech compactification of the integers) proved using CH have a more general version proved using only MA. Baire category and measure theory theorems proved traditionally for countable sets can often be extended to sets of cardinality less than 2^ω . And in any field of mathematics when one would like to prove a theorem for ω_1 sets and one knows an inductive proof of the theorem for countable sets, there is a natural setup for applying $(\text{MA} + \neg \text{CH})$. The difficulty is in proving that this natural partial order is ccc. It may not be ccc, in which case MA may not be applicable.

References

MARTIN, D.A. and SOLOVAY, R.

[1970] Internal Cohen extensions, *Ann. Math. Logic*, **2**, 143–178.

EKLOF, P.C.

[1977] Whitehead's problem is undecidable, *Am. Math. Monthly* (to appear).

SHOENFIELD, J.

[1975] Martin's axiom, *Am. Math. Monthly*, **82** (6), 610–617.

Consistency Results in Topology

I. JUHÁSZ

Contents

Introduction	504
1. Applications of Martin's axiom	504
2. Combinatorial principles valid in L	510
References	522

Introduction

It is not at all surprising that developments in set theory affect topology. This is true about the theory of the most familiar topological spaces, like that of the reals and of its subspaces, as well as about the general theory of topological spaces. The most striking examples in the first area are the recent advances in descriptive set theory (discussed in Chapter C.8) while the purpose of the present paper is to exhibit results of the second sort.

The underlying theme of the paper is to introduce certain set-theoretic assumptions (like Martin's axiom, $\diamond$, etc.) unearthed by set theorists (who have proved their consistency) and then illustrate how these can be used in proving topological theorems or constructing counterexamples. This we do without worrying about how the actual consistency of these principles is established. There is really nothing strange, or even new, in this practice; think of the numerous results obtained with the use of the continuum hypothesis by people who had no idea how to prove its consistency (or did not even know it was consistent).

There are several reasons for the promotion of this practice among topologists. First of all, it turns out to be "nice mathematics", so it serves the aesthetic pleasure of those fond of set-theoretic methods. Secondly, by accumulating "data", it might contribute to the better understanding of the "nature" of set theory itself.

The notation used in this paper follows Chapter B.3 and JUHÁSZ [1971]; one exception is the tightness which is denoted by $\iota(X)$ instead of $\partial(X)$. Also the notion of the π -character $\pi\chi(p, X)$ of a point p in a space X is not defined there, it is the smallest cardinal of a family $\mathcal{P}$ of non-empty open sets in X such that every neighborhood of p contains a member of $\mathcal{P}$. (We recall that a π -base $\mathcal{P}$ for a space is the global analogue of this, i.e., a family of non-empty open sets such that every non-empty open set contains a member of $\mathcal{P}$, while the π -weight $\pi(X)$ of a space X is the smallest cardinal of a global π -base for X .)

We shall say that a space is κ -Baire if it can not be written as the union of less than κ nowhere dense subsets. 2^ω -Baire spaces are also called strongly Baire.

1. Applications of Martin's axiom

1.1. π -completeness

As is shown, e.g. in MARTIN and SOLOVAY [1970], MA is equivalent to the

statement that every compact T_2 space with the Suslin property satisfies the strong Baire property, i.e. is not the union of less than 2^ω nowhere dense subsets. It turns out that compactness can be replaced by a much more general “completeness” property here, which is not surprising since we know that the Baire property is more closely related to completeness than to compactness.

The property we are about to introduce is quite general, it includes e.g. all Čech-complete spaces as well as all almost subcompact spaces (cf. AARTS and LUTZER [1974]). We recall that a filter base $\mathcal{F}$ in a space X is called regular if $F_1, F_2 \in \mathcal{F}$ implies the existence of $F \in \mathcal{F}$ such that $\bar{F} \subset \text{Int}(F_1 \cap F_2)$.

DEFINITION. A regular space X is called π -complete if it has a family $\{\mathcal{P}_\alpha: \alpha < \lambda\}$ of π -bases with $\lambda < 2^\omega$ such that whenever $\mathcal{F} \subset \bigcup \{\mathcal{P}_\alpha: \alpha < \lambda\}$ is a regular filter base with $|\mathcal{F}| < 2^\omega$ and $\mathcal{F} \cap \mathcal{P}_\alpha \neq \emptyset$ for each $\alpha < \lambda$, then $\bigcap \mathcal{F} \neq \emptyset$.

Remark. The restriction to regular spaces is not essential, everything below goes through without regularity if instead of π -bases we would take families of open sets with the property that every non-empty open set contains the closure of a member of them.

1.2. THEOREM (MA). *Every π -complete space X with the Suslin property (i.e., with $c(X) = \omega$) has the strong Baire property.*

PROOF. Let $\{\mathcal{P}_\alpha: \alpha < \lambda\}$ be the family of π -bases required for π -completeness and put $\mathcal{P} = \bigcup \{\mathcal{P}_\alpha: \alpha < \lambda\}$. We define a partial order $<$ on $\mathcal{P}$ by letting $P < Q$ iff $\bar{P} \subset Q$ and $P \neq Q$. Clearly, $\langle \mathcal{P}, < \rangle$ is a CCC partial order.

Now let $\kappa < 2^\omega$ and assume that $\{A_\xi: \xi < \kappa\}$ are nowhere dense subsets of X . We shall show that $X \neq \bigcup \{A_\xi: \xi < \kappa\}$. For every $\alpha < \lambda$ and $\xi < \kappa$ let

$$D_{\alpha, \xi} = \{P \in \mathcal{P}_\alpha: P \cap A_\xi = \emptyset\}.$$

It is easy to see that every $D_{\alpha, \xi}$ is dense in the partially ordered set $\langle \mathcal{P}, < \rangle$. So by MA there exists $\mathcal{G} \subset \mathcal{P}$ which is generic over the family $\{D_{\alpha, \xi}: \alpha < \lambda, \xi < \kappa\}$. Genericity in $\langle \mathcal{P}, < \rangle$ obviously implies that $\mathcal{G}$ is a regular filter base in X which intersects every $\mathcal{P}_\alpha$ for $\alpha < \lambda$ and has a member missing A_ξ for every $\xi < \kappa$. Now an easy “Löwenheim–Skolem type” (see Chapter A.2) argument yields us a regular filter base $\mathcal{F} \subset \mathcal{G}$ with $|\mathcal{F}| < 2^\omega$ and having

the above properties of $\mathcal{G}$. By the definition of π -completeness we have then

$$\emptyset \neq \bigcap \mathcal{F} \subset X \setminus \bigcup \{A_\xi : \xi < \kappa\},$$

which proves the theorem. Let us remark that if $2^\omega = \omega_1$ (i.e. CH holds) then the result remains valid without the assumption $c(X) = \omega$. $\square$

COROLLARY (MA). *If X is π -complete and $c(X) = \omega$, then X^ω has the strong Baire property.*

PROOF. If $\{\mathcal{P}_\alpha : \alpha < \lambda\}$ is a suitable family of π -bases for X , let us define $\mathcal{P}_{\alpha,n}$ for $\alpha < \lambda$ and $n < \omega$ as the set of all elementary open subsets of the product X^ω of the form

$$\bigcap \{\pi_i^{-1}(P_i) : i \in I\},$$

where $I \in [\omega]^{<\omega}$, $P_i \in \mathcal{P}_\alpha$ for each $i \in I$, and $n \in I$. Then each $\mathcal{P}_{\alpha,n}$ is a π -base of X^ω , moreover it follows easily from the definitions that if $\mathcal{F} \subset \bigcup \{\mathcal{P}_{\alpha,n} : \alpha < \lambda, n < \omega\}$ is a regular filter base with $|\mathcal{F}| < 2^\omega$ and $\mathcal{F} \cap \mathcal{P}_{\alpha,n} \neq \emptyset$ for each α and n , then $\mathcal{F}_n = \{\pi_n(P) : P \in \mathcal{F}\}$ is a regular filter base contained in $\bigcup \{\mathcal{P}_\alpha : \alpha < \lambda\}$ intersecting every $\mathcal{P}_\alpha$ and having $|\mathcal{F}_n| < 2^\omega$, consequently $\bigcap \mathcal{F}_n = \bigcap \{\pi_n(P) : P \in \mathcal{F}\} \neq \emptyset$ for each $n < \omega$, hence $\bigcap \mathcal{F} \neq \emptyset$. This shows that X^ω is π -complete. If CH fails we also have $c(X^\omega) = \omega$ by Theorem 6 of Chapter B.6 on MA and the fact that $c(X) = \omega$. Thus we can apply Theorem 1.2 and the remark at the end of its proof to conclude that X^ω has the strong Baire property. $\square$

The following result does not use MA and thus might be of interest in itself.

1.3. THEOREM. *Let X be any space and κ be an infinite cardinal. If X^ω is κ -Baire and $\pi(X) < \kappa$, then $d(X) = \omega$ (i.e. X is separable).*

PROOF. Let $\mathcal{P}$ be a π -base for X with $|\mathcal{P}| < \kappa$. For any fixed $P \in \mathcal{P}$ let $\mathcal{G}_P$ be the family of all elementary open subsets of X^ω one of whose factors is equal to P , i.e.,

$$\mathcal{G}_P = \left\{ \bigcap_{i \in I} \pi_i^{-1}(G_i) : I \in [\omega]^{<\omega} \text{ \& \& } \exists i \in I \text{ s.t. } G_i = P \right\}.$$

Clearly, $\mathcal{G}_P$ is a π -base for X^ω , hence $D_P = \bigcup \mathcal{G}_P$ is a dense open subset of X^ω . By the κ -Baire property of X^ω we have $D = \bigcap \{D_P : P \in \mathcal{P}\} \neq \emptyset$, so

let $x \in D$. We claim that $S = \{x_n = \pi_n(x) : n \in \omega\}$ is dense in X . Indeed, let $G \subset X$ be an arbitrary non-empty open set in X . Then there is $P \in \mathcal{P}$ with $P \subset G$, and since $x \in D_P$ there is $n \in \omega$ such that $\pi_n(x) = x_n \in P \subset G$, proving that S is dense in X , hence $d(X) = \omega$. $\square$

COROLLARY (MA). *If X is π -complete, $c(X) = \omega$, and $\pi(X) < 2^\omega$, then $d(X) = \omega$.*

PROOF. The proof is immediate from Corollary 1.2 and Theorem 1.3.

1.4. REMARK. This last result is the basis for proving a number of theorems of the following kind: $(MA + \neg CH)$ implies that if X is complete, Suslin and has “small” local characters, then X is separable (cf. HAJNAL and JUHÁSZ [1971], ŠAPIROVSKII [1972], TALL [1974]). The next result is a very general one of this sort. We omit its proof because it uses only “conventional” techniques to deduce the result from the Corollary to Theorem 1.3.

THEOREM (MA). *Suppose X is such that*

- (i) *every closed subspace of X is π -complete;*
- (ii) $c(X) = \omega$;
- (iii) $t(X)^+ < 2^\omega$ and $\pi\chi(p, X) < 2^\omega$ for every $p \in X$.

Then X is separable.

Čech-complete spaces are examples of spaces satisfying (i). Šapirovsii proved (unpublished) that for X compact, $\pi\chi(X) \leq t(X)$. Therefore as a consequence of the above theorem we get: $(MA + \neg CH)$ implies that if X is compact, Suslin and $t(X) = \omega$, then X is separable. It is not known whether $t(X) = \omega$ could be replaced by $\pi\chi(X) = \omega$ in this result.

The previous results seem to need the “full force” of MA, while the ones we shall look at below all depend on a combinatorial consequence of MA that is known to be strictly weaker than MA (cf. KUNEN and TALL [1977]).

So let us recall (Theorem 8 of Chapter B.6) that the following proposition is a consequence of MA:

- (*) If $\mathcal{A} \subset \mathcal{P}(\omega)$, $|\mathcal{A}| < 2^\omega$ and $|\bigcap \mathcal{B}| = \omega$ whenever $\mathcal{B} \subset \mathcal{A}$ is finite, then there is an infinite $S \subset \omega$ such that $S \setminus A$ is finite for all $A \in \mathcal{A}$ (i.e. S is almost contained in every member of $\mathcal{A}$).

The following result is an immediate consequence of this proposition.

1.5. THEOREM (MA; cf. HECHLER [1976]). *Let X be a separable and countably compact space and $\mathcal{U}$ be an open cover of X with $|\mathcal{U}| < 2^\omega$. Then there is a finite subfamily $\mathcal{V} \subset \mathcal{U}$ such that $\bigcup \mathcal{V}$ is dense in X .*

PROOF. Let $S \subset X$ be a countable dense subset of X and assume that $\mathcal{U}$ has no finite subset $\mathcal{V}$ with dense union. Then the family

$$\mathcal{A} = \{S \setminus U : U \in \mathcal{U}\}$$

of subsets of S clearly has the property that any intersection of finitely many members of $\mathcal{A}$ is infinite. Hence using (*) we can find an infinite subset $C \subset S$ with $C \setminus (S \setminus U) = C \cap U$ finite for each $U \in \mathcal{U}$. But then C can have no limit point in X , since $\mathcal{U}$ is a cover, which contradicts the countable compactness of X . $\square$

The next result of W. Weiss follows from Theorem 1.5, and is especially interesting because of a later result that “confronts” it.

1.6. THEOREM (MA + $\neg$ CH). *Every countably compact, perfect, and regular space X is compact.*

PROOF. It is sufficient, of course, to show that X is Lindelöf. So assume, striving for a contradiction, that X is not Lindelöf. It is shown e.g. in STEPHENSON [1972] that a perfect and countably compact space has countable spread, i.e. $s(X) = \omega$. Since X is not Lindelöf, it contains a right-separated subset $R = \{p_\xi : \xi < \omega_1\}$ of type ω_1 , moreover $s(R) = s(X) = \omega$ implies that R is actually hereditarily separable (cf. JUHÁSZ [1971]). For each $\xi < \omega_1$ there is a neighborhood U_ξ of p_ξ in X with $p_\eta \notin \bar{U}_\xi$ for $\eta > \xi$, where the regularity of X is also taken into account. Since X is perfect, the open set $G = \bigcup \{U_\xi : \xi < \omega_1\}$ is an F_σ , hence there are closed sets $\{F_n : n < \omega\}$ such that $G = \bigcup \{F_n : n < \omega\}$. There is an $n_0 < \omega$ then with $|R \cap F_{n_0}| = \omega_1$.

Let us put $Z = R \cap F_{n_0}$, then Z is countably compact being closed in X and separable because its dense subset $R \cap F_{n_0}$ is. Finally $\mathcal{U} = \{U_\xi : \xi < \omega_1\}$ is an open cover of Z with $|\mathcal{U}| < 2^\omega$, hence Hechler's theorem can be applied and yields us a finite

$$\mathcal{V} = \{U_{\xi_1}, \dots, U_{\xi_n}\} \subset \mathcal{U} \quad \text{such that} \quad Z \subset \bigcup_{k=1}^n \bar{U}_{\xi_k}.$$

But if ξ_j is the largest among the ξ_k ($k = 1, \dots, n$) then this union contains no p_η with $\eta > \xi_j$, contradicting that the uncountable set $R \cap F_{n_0}$ should be contained in it. $\square$

Finally, we look at some completely different consequences of this same combinatorial principle. The following result is due to MALYHIN and ŠAPIROVSKII [1973].

1.7. THEOREM (MA). *Let X be any space and $p \in X$ and $S \subset X$ be such that $p \in \bar{S} \setminus S$ and $|S| = \omega$. Then there is a sequence of points from S converging to p provided that either of the following two conditions is satisfied:*

- (i) $\chi(p, \bar{S}) < 2^\omega$;
- (ii) X is regular, countably compact, and $\psi(p, \bar{S}) < 2^\omega$.

PROOF. We can assume, without loss of generality, $X = \bar{S}$. Now let $\mathcal{U}$ with $|\mathcal{U}| < 2^\omega$ be a system of neighborhoods of p in X such that $\mathcal{U}$ is a neighborhood basis for p if (i) holds, or

$$\bigcap \{\bar{U} : U \in \mathcal{U}\} = \{p\}$$

if (ii) holds. Next we define a family $\mathcal{A}$ of subsets of S by putting

$$\mathcal{A} = \{U \cap S : U \in \mathcal{U}\}$$

if case (i) holds, and

$$\mathcal{A} = \{\bar{U} \cap S : U \in \mathcal{U}\}$$

if case (ii) holds. Clearly, any finite intersection of members of $\mathcal{A}$ is infinite in both cases, since p cannot be isolated. Therefore proposition (*) can again be applied to obtain an infinite subset $M \subset S$, $M = \{q_n : n < \omega\}$ such that $M \setminus U$ is always finite in case (i), and $M \setminus \bar{U}$ is always finite in case (ii). This of course immediately implies that the sequence q_n converges to p in case (i), or that it has no limit point in $X \setminus \{p\}$ if case (ii) holds. But X being countably compact in this case, p is the unique limit point of q_n , hence it must converge to p , as follows immediately from the countable compactness of X again.

COROLLARY 1 (MA). *Any compact space of cardinality less than 2^{2^ω} is sequentially compact.*

PROOF. Let $S \subset X$ be any countably infinite set. If $\bar{S} = S$, we can obviously select a convergent sequence from S . So we have $S \setminus \bar{S} \neq \emptyset$. Using the Čech–Pospíšil theorem (4.3 of Chapter B.3) there is a $p \in \bar{S} \setminus S$ with $\chi(p, \bar{S}) < 2^\omega$, since otherwise we would have $|S| \geq 2^{2^\omega} > |X|$, a contradiction. Thus by case (i) of Theorem 1.7 a convergent sequence can again be selected from S . $\square$

COROLLARY 2 (MA). *If X is regular, extremally disconnected, and separable, then every non-isolated point of it has character $\geq 2^\omega$, and if X is also countably compact we have $\psi(p, X) \geq 2^\omega$ for p non-isolated in X .*

Indeed, this follows immediately from Theorem 1.7 and the fact that in a regular extremally disconnected space there is no non-trivial convergent sequence. As an example of this, we have $\chi(p, \beta N) = 2^\omega$ for every $p \in \beta N \setminus N$ (under MA).

2. Combinatorial principles valid in L

While MA has, by now, become an accessible tool for the classical mathematicians (especially popular among topologists), the combinatorial principles that we are going to illustrate in this section are considerably less well known among non-logicians. It is true that they are more recent and look more complicated than MA, but we hope their consequences are interesting enough to convince the reader about their usefulness. It is an interesting phenomenon (also mentioned in Chapter B.6) that these principles often work in the opposite direction from $\text{MA} + \neg \text{CH}$. They also have an advantage which MA does not have: they easily generalize to most higher cardinals. As to their origin and consistency, they are all “byproducts” of the (profound) investigations into the “fine structure” of L, the constructible universe, carried out mostly by R. Jensen (cf. Chapter B.5 on L), however their consistency is usually established more easily using “simple” forcing (cf. Chapter B.4 on forcing).

2.1. The principle $\diamond$

We use $\diamond$ to abbreviate the following statement:

We can simultaneously associate to every $\alpha < \omega_1$ an $S_\alpha \subset \alpha$ such that whenever $S \subset \omega_1$ the set $\{\alpha < \omega_1: S \cap \alpha = S_\alpha\}$ is stationary in ω_1 . We refer to the discussion of stationary sets, in Section 2 of Chapter B.3, where it is also shown that $\diamond \rightarrow \text{CH}$ and $\diamond \rightarrow \neg \text{SH}$.

In what follows we construct, using $\diamond$, a small Dowker space with many nice properties. The main idea is to ally the construction in OSTASZEWSKI [1975] of a hereditarily separable, locally compact, countably compact and perfectly normal non-compact space with the basic trick of RUDIN [1955]. In this latter paper it is shown that the existence of a Suslin tree (i.e. $\neg \text{SH}$) implies that of a small Dowker space. Since $\diamond \rightarrow \neg \text{SH}$, our result is not too surprising, even if we take into account the nice additional properties

that our Dowker space possesses. The reason we are giving it here is to publicize the method of construction rather than the result itself.

Let us note now that the sequence $\langle S_\alpha : \alpha < \omega_1 \rangle$ in the definition of $\Diamond$ has the following property:

- (+) If $A \subset \omega_1$ is uncountable, then there is a limit ordinal $\lambda < \omega_1$ such that $S_\lambda \subset A$ and $\bigcup S_\lambda = \lambda$ (i.e. S_λ is cofinal in λ).

Indeed, since A is unbounded, A' , the set of its limit points is closed and unbounded. Therefore $A' \cap \{\alpha : A \cap \alpha = S_\alpha\} \neq \emptyset$, and clearly any λ from this intersection will satisfy (+). Put L_1 to denote the set of all limit ordinals in ω_1 , moreover put for each $\lambda \in L_1$

$$T_\lambda = \begin{cases} S_\lambda & \text{if } \bigcup S_\lambda = \lambda; \\ \lambda & \text{if } \bigcup S_\lambda < \lambda. \end{cases}$$

Then every T_λ is cofinal in λ and clearly $\langle T_\lambda : \lambda \in L_1 \rangle$ also has property (+).

2.2. THEOREM ($\Diamond$). *There exists a topology τ on $\omega_1 \times \omega$ with the following properties:*

- (i) τ is locally compact and Hausdorff;
- (ii) τ is locally countable;
- (iii) τ is hereditarily separable;
- (iv) τ is normal;
- (v) τ is not countably paracompact.

PROOF. Let us introduce some notation first. For $\lambda \in L_1$ put $X_\lambda = \lambda \times \omega$ and $X = \bigcup \{X_\lambda : \lambda \in L_1\} = \omega_1 \times \omega$. Since $\Diamond \rightarrow \text{CH}$, we can arrange all countable subsets of X in a sequence $\langle A_\lambda : \lambda \in L_1 \rangle$, where we may also assume that each A_λ is a bounded subset of X_λ , i.e. that $A_\lambda \subset \alpha \times \omega$ for some $\alpha < \lambda$. Finally, for every $\langle \alpha, n \rangle \in X$ define

$$B(\alpha, n) = [\alpha \times (n+1)] \cup \{\langle \alpha, n \rangle\},$$

$$C(\alpha, n) = (\omega_1 \setminus \alpha) \times (\omega \setminus n).$$

To define τ , we shall first define by induction on $\lambda \in L_1$ topologies τ_λ and sets Z_λ for every $\lambda \in L_1$ as follows.

Suppose $\lambda \in L_1$ and we have already defined a topology τ_σ on X_σ and a set $Z_\sigma \subset X_\sigma$ for each $\sigma \in \lambda \cap L_1$ such that the following inductive hypotheses are satisfied:

- (1) τ_σ is locally compact and T_2 ;

(2) if $\rho, \sigma \in \lambda \cap L_1$ and $\rho < \sigma$ then $\langle X_\rho, \tau_\rho \rangle$ is an open subspace of $\langle X_\sigma, \tau_\sigma \rangle$;

(3) for every $\langle \alpha, n \rangle \in X_\sigma$ the set $B(\alpha, n)$ is τ_σ -open;

(4) for all $\rho, \sigma \in \lambda \cap L_1$ with $\rho \leq \sigma$, Z_ρ is a bounded τ_σ -clopen subset of X_ρ .

Now if λ is a limit of limits ($\lambda \in L'_1$), then we are forced by (2) to take $\bigcup \{\tau_\sigma : \sigma \in \lambda \cap L_1\}$ as a basis for τ_λ on X_λ , and it is quite obvious that (1)–(3) will remain valid for τ_λ as well. Moreover since any Z_ρ is τ_σ -clopen by (4) if $\rho, \sigma \in \lambda \cap L_1$, $\rho \leq \sigma$, we get that Z_ρ also remains τ_λ -clopen. (Indeed, this follows immediately from $X_\lambda \setminus Z_\rho = \bigcup \{X_\sigma \setminus Z_\rho : \sigma \in \lambda \cap L_1\}$).

If on the other hand $\lambda \notin L'_1$, i.e. $\lambda = \sigma + \omega$ for some $\sigma \in L_1$ then we have to do some work to define basic neighborhoods for the new points in $X_\lambda \setminus X_\sigma$. To do that, first arrange the members of the countable family $\{Z_\rho : \rho \in \lambda \cap L_1\}$ in an ω -type sequence $\langle Z^{(n)} : n \in \omega \rangle$, and then consider the set T_σ which by our choice is cofinal in σ . Pick a strictly increasing cofinal sequence $G^{(\sigma)} = \{\gamma_t : t \in \omega\} \subset T_\sigma$. For every $\langle \alpha, n \rangle \in X_\sigma$ we have then

$$|B(\alpha, n) \cap (G^{(\sigma)} \times \omega)| < \omega,$$

hence by (3), the set $G^{(\sigma)} \times \omega$ has no limit point in $\langle X_\sigma, \tau_\sigma \rangle$. But then using the fact that $\langle X_\sigma, \tau_\sigma \rangle$ is a countable locally compact T_2 space (and therefore 0-dimensional metrizable) we can select *compact open* τ_σ -neighborhoods $K_{t,s}$ of the points $\langle \gamma_t, s \rangle$ in $G^{(\sigma)} \times \omega$ which are pairwise disjoint, satisfy $K_{t,s} \subset B(\gamma_t, s)$ for every $t, s \in \omega$, and also have the property that for any $t, s \in \omega$ if $\langle \gamma_t, s \rangle \notin Z^{(l)}$, then $K_{t,s} \cap Z^{(l)} = \emptyset$ for all $l < t$. This last condition can be met since each $Z^{(l)}$ is τ_σ -clopen.

Now let us partition ω into disjoint infinite sets as follows:

$$\omega = \bigcup \{a_{n,m} : n, m \in \omega\},$$

$a_{n,m} \cap a_{n',m'} = \emptyset$ if $\langle n, m \rangle \neq \langle n', m' \rangle$, and $|a_{n,m}| = \omega$ for every $n, m \in \omega$. Every point of $X_\lambda \setminus X_\sigma$ is of the form $\langle \sigma + n, m \rangle$. We define the k -th neighborhood $V_k(\sigma + n, m)$ of this point by

$$V_k(\sigma + n, m) = \bigcup \{K_{t,s} : t \in a_{n,m} \setminus k \text{ and } s \leq m\} \cup \{\langle \sigma + n, m \rangle\}.$$

It is immediate from this definition that these countable neighborhoods together with τ_σ generate a Hausdorff topology τ_λ on X_λ of which $\langle X_\sigma, \tau_\sigma \rangle$ is an open subspace. It is also easy to see that every $V_k(\sigma + m, n)$ is compact in $\langle X_\lambda, \tau_\lambda \rangle$ because any infinite subset of it is either covered by finitely many of the (compact) sets $K_{t,s}$ forming $V_k(\sigma + m, n)$, or intersects infinitely many of them, and so in either case it has a limit point. We also have $V_0(\sigma + n, m) \subset B(\sigma + n, m)$ by the construction. Finally, given any

$\rho \leq \sigma$, we have $Z_\rho = Z^{(l)}$ for some $l \in \omega$. But $Z^{(l)}$ is bounded in X_σ and at the same time $G^{(\omega)}$ converges to σ , hence for each $s \in \omega$ we have $\langle \gamma_s, s \rangle \notin Z^{(l)}$ for large enough $t \in \omega$. But by our construction then we also have $V_k(\sigma + m, n) \cap Z^{(l)} = \emptyset$ for large enough k , for any fixed $m, n \in \omega$, hence no point of $X_\lambda \setminus X_\sigma$ is a limit point of $Z_\rho = Z^{(l)}$, which thus remains τ_λ -clopen.

Now it only remains to define Z_λ for both types of λ . To this end consider the set A_λ . If A_λ is not τ_λ -closed, simply put $Z_\lambda = \emptyset$. If it is τ_λ -closed pick first an $\alpha \in \lambda$ with $A_\lambda \subset \alpha \times \omega$. Since (3) is valid, clearly $\alpha \times \omega$ is τ_λ -open, hence using again the obvious fact that $\langle X_\lambda, \tau_\lambda \rangle$ is a countable metrizable space we can pick a τ_λ -clopen set Z_λ such that $A_\lambda \subset Z_\lambda \subset \alpha \times \omega$. This completes the induction.

Let τ be the topology on X generated by $\bigcup \{\tau_\lambda : \lambda \in L_1\}$. We claim that (i)–(v) are satisfied by $\langle X, \tau \rangle$. (i) and (ii) follow immediately from the hypotheses (1) and (2). To see the rest we first establish property (vi) which is interesting in its own right.

(vi) *For every $\sigma \in L_1$ and $n \in \omega$ we have $\text{cl}_\tau(T_\sigma \times \{n\}) \supset C(\sigma, n)$.*

To prove this, note first of all that

$$\text{cl}_\tau(T_\sigma \times \{n\}) \supset (\sigma + \omega \setminus \sigma) \times (\omega \setminus n)$$

is immediate from our construction, since every point $\langle \sigma + m, n' \rangle$ is in the τ -closure of $G^{(\omega)} \times \{n\} \subset T_\sigma \times \{n\}$ for $n' \geq n$. Next we prove by induction on the members λ of $L_1 \setminus \sigma$ that $\langle \lambda + m, n' \rangle \in \text{cl}_\tau(T_\sigma \times \{n\})$ if $n' \geq n$. We have just established this for $\lambda = \sigma$, now assume $\lambda \in L_1 \setminus (\sigma + \omega)$ and that the inductive hypothesis is valid for $\lambda' \in L_1$ with $\sigma \leq \lambda' < \lambda$. But the same argument as for the initial case of σ yields us

$$\langle \lambda + m, n' \rangle \in \text{cl}_\tau(G^{(\lambda)} \times \{n\})$$

whenever $n' \geq n$, moreover $G^{(\lambda)} \cap \sigma$ is finite by its definition, hence using the inductive hypothesis for the members of $(G^{(\lambda)} \setminus \sigma) \times \{n\}$ we get

$$\langle \lambda + m, n' \rangle \in \text{cl}_\tau((G^{(\lambda)} \setminus \sigma) \times \{n\}) \subset \text{cl}_\tau(T_\sigma \times \{n\}),$$

as was required.

Now we first show that (iii) is valid. Indeed, let $Y \subset X$ be uncountable and n be minimal such that $Y \cap [\omega_1 \times \{n\}]$ is uncountable. Then by (+) there is $\sigma \in L_1$ such that $T_\sigma \times \{n\} \subset Y$. By the choice of n we have that $Y \cap [\omega_1 \times n]$ is countable, hence using (vi) we get that

$$(Y \cap [\omega_1 \times n]) \cup (T_\sigma \times \{n\}) \cup (Y \cap X_\sigma)$$

is a countable τ -dense subset of Y .

To see that (iv) is satisfied let us note first of all that the above argument also yields us that any uncountable τ -closed subset of X contains a set of the form $C(\sigma, n)$. But clearly $C(\sigma, n) \cap C(\sigma', n') \neq \emptyset$ for any $\sigma, \sigma' \in \omega_1$, $n, n' \in \omega$. Hence if H and K are two disjoint τ -closed sets in X then at least one of them, say H , is countable. Then $H = A_\lambda$ for some $\lambda \in L_1$, moreover Z_λ is a τ -clopen set such that $H = A_\lambda \subset Z_\lambda \subset \alpha \times \omega$ for some $\alpha < \lambda$.

Now H and $K \cap X_\lambda$ are disjoint τ , and therefore τ_λ -closed subsets of X_λ , hence there are disjoint τ_λ - and therefore τ -open sets U and V in X_λ such that $H \subset U$ and $K \cap X_\lambda \subset V$. But then $U \cap Z_\lambda$ and $V \cup (X \setminus Z_\lambda)$ are disjoint τ -open neighborhoods of H and K respectively, showing that $\langle X, \tau \rangle$ is indeed normal.

To see (v), consider the sets $F_n = C(0, n) = \omega_1 \times (\omega \setminus n)$ for each $n \in \omega$. Clearly $F_0 \supset F_1 \supset \dots$, $\bigcap \{F_n : n \in \omega\} = \emptyset$, and each F_n is τ -closed, hence it suffices to show that given any sequence $\langle G_n : n \in \omega \rangle$ of τ -open sets such that $G_n \supset F_n$ for each $n \in \omega$, then $\bigcap \{G_n : n \in \omega\} \neq \emptyset$. In fact we claim that for any $n \in \omega$ and any τ -open set $G_n \supset F_n$ we have $[\omega_1 \times \{0\}] \setminus G_n$ is countable. Suppose, on the contrary that this set is uncountable. From the proof of (vi) we get then that the τ -closed set $X \setminus G_n \supset C(\sigma, 0)$ for some $\sigma \in \omega_1$, which however contradicts $G_n \supset F_n = C(0, n)$. $\square$

Remark. The reader familiar with Ostaszewski's construction (cf. also RUDIN [1974]) can easily convince himself that without much trouble we could have also achieved that the subspace $\omega_1 \times n$ of $\langle X, \tau \rangle$ be countably compact for each $n \in \omega$, hence X be σ -countably compact. Another refinement of the method allows one to construct a nice small Dowker space with the aid of CH only (cf. JUHÁSZ, KUNEN and RUDIN [1977]), but then local compactness and σ -countably compactness have to be abandoned.

Ideas of this construction will also appear in 2.9.

2.3. Proposition W

The combinatorial principle under consideration in this section is really an offspring of Jensen's "morass" (cf. DEVLIN [1973]). Its relevance to topology is well illustrated by the fact that it was originally designed by J. Silver to replace the "morass" in some constructions used to get large S-spaces in the constructible universe. In case the reader finds this principle W too complicated, he is advised to look up the definition of a morass.

We shall actually generalize somewhat Silver's W by introducing a

cardinal parameter into it. ($W = W(\omega_2)$.) So let κ be an infinite cardinal, we shall use $W(\kappa)$ to denote the following statement:

There exists a tree T of height $\omega_1 + 1$ with the following properties (i)–(iii) (we use T_α to denote the α -th level of T and p_α to denote the function assigning to every $t \in T_\beta$ with $\beta \geq \alpha$ the (unique) predecessor of t at level α):

- (i) $|T_{\omega_1}| = \kappa$ and $|T_\alpha| \leq \omega$ for $\alpha < \omega_1$;
- (ii) if $s, t \in T_{\omega_1}$, $s \neq t$, then $p_\alpha(s) \neq p_\alpha(t)$ for some $\alpha < \omega_1$;
- (iii) there exists a sequence $\{w_\alpha : \alpha < \omega_1\}$ with each w_α a countable family of countably infinite subsets of T_α such that (*) for every $A \in [T_{\omega_1}]^\omega$ there is an $\alpha_A < \omega_1$ with $p_\alpha(A) \in w_\alpha$ if $\alpha_A \leq \alpha < \omega_1$.

Now, it is not hard to show that both $W(\omega)$ and $W(\omega_1)$ are equivalent to CH. It is also easy to see that $W(\kappa)$ implies $\kappa \leq 2^{\omega_1}$ because $|\bigcup \{T_\alpha : \alpha < \omega_1\}| = \omega_1$ and different members of T_{ω_1} have different sets of predecessors. A standard forcing argument will show that, on the other hand (ZFC + 2^{ω_1} is arbitrarily large + $W(2^{\omega_1})$) is consistent (cf. Chapter B.4). The really tough thing is to show that $W(\omega_2) = W(2^{\omega_1})$ holds in L; this was done by Silver.

2.4. DEFINITION. An infinite subset $X \subset D(2)^{\omega_1}$ (here $D(2)$ is just the discrete space on $2 = \{0, 1\}$) is called an HFD-set (short for hereditarily finally dense) if the following condition (**) is satisfied:

- For every $A \in [X]^\omega$ there exists a $\nu_A < \omega_1$ such that
- (**) whenever ε is any finite partial function from $\omega_1 \setminus \nu_A$ into 2 there is $f \in A$ with $\varepsilon \subset f$.

Informally (**) says that the “tails” of the functions in A are dense in the partial product $D(2)^{\omega_1 \setminus \nu_A}$.

2.5. THEOREM. If $W(\kappa)$ holds, then there is an HFD-set $X \subset D(2)^{\omega_1}$ with $|X| = \kappa$.

PROOF. Let T and $\{w_\alpha : \alpha < \omega_1\}$ be as required in the definition of $W(\kappa)$. Let us introduce the following technical definition: for any $S \in w_\alpha$ put

$$\beta(S) = \min\{\beta : \forall \gamma [(\beta \leq \gamma \leq \alpha) \Rightarrow p_\gamma(S) \in w_\gamma \text{ and } p_\gamma \upharpoonright S \text{ is 1-1}]\}.$$

Clearly, $\beta(S) \leq \alpha$. Now, our aim is to define functions $f^t : \alpha + 1 \rightarrow 2$ for every $t \in T_\alpha$ ($\alpha < \omega_1$) by induction on α so that they approximate the members of our purported set X . So assume that $\alpha < \omega_1$ and we have

already defined the functions $f^t : \beta + 1 \rightarrow 2$, for $t \in T_\beta$ and $\beta < \alpha$, satisfying the following inductive hypotheses:

$$\text{if } \gamma < \beta < \alpha \text{ and } t \in T_\beta, \text{ then } f^t \supset f^{p_\gamma(t)}; \quad (1)$$

if $S \in w_\beta$ and ε is a finite function from a subset of $(\beta + 1) \setminus \beta(S)$ into 2, then the set $S_\varepsilon = \{t \in S : \varepsilon \subset f^t\}$ is infinite. (2)

Next we have to define f^t if $t \in T_\alpha$. The only problem, of course, is to define $f^t(\alpha)$, since for any $\beta < \alpha$ we have to put

$$f^t(\beta) = f^{p_\beta(t)}(\beta)$$

if we want to keep (1) valid for α . So let $Z(\alpha)$ be the family of all infinite sets of the form S_ε , where $S \in w_\alpha$ and ε is a finite function from $\alpha \setminus \beta(S)$ into 2. This makes sense because $f^t(\beta)$ has already been defined for all $\beta < \alpha$. Let us note that we have $S_\emptyset = S$ for the empty function, hence $w_\alpha \subset Z(\alpha)$. Now the family $Z(\alpha)$ is a countable family of countably infinite subsets of T_α , hence by Bernstein's well-known theorem we can split T_α into two disjoint sets $H_0^{(\alpha)}$ and $H_1^{(\alpha)}$ so that

$$|S_\varepsilon \cap H_i^{(\alpha)}| = \omega$$

for every $S_\varepsilon \in Z(\alpha)$ and $i < 2$. Then we define $f^t(\alpha)$ by putting

$$f^t(\alpha) = \begin{cases} 0 & \text{if } t \in H_0^{(\alpha)}; \\ 1 & \text{if } t \in H_1^{(\alpha)}. \end{cases}$$

It is clear from this definition that (2) is also satisfied for α , hence the induction goes through. So we can define for each $s \in T_{\omega_1}$ a function $f_s \in D(2)^{\omega_1}$ as follows

$$f_s = \bigcup \{f^{p_\alpha(s)} : \alpha < \omega_1\}.$$

Then it only remains to check that $X = \{f_s : s \in T_{\omega_1}\} \subset D(2)^{\omega_1}$ is indeed HFD. To see that let $A \in [T_{\omega_1}]^\omega$ be arbitrary and choose $\alpha < \omega_1$ so that $p_\alpha \upharpoonright A$ is 1-1 and $p_\gamma(A) \in w_\gamma$ for all $\gamma \geq \alpha$, which is possible by (*). Now it is clear from (1) and (2) that $\beta(p_\alpha(A))$ will work as ν_A , as required in (**). $\square$

2.6. REMARKS. It is shown in HAJNAL and JUHÁSZ [1974] that an HFD subspace X of $D(2)^{\omega_1}$ is always hereditarily separable and hereditarily normal. Now it is also immediate that if for every $f \in X$ we have $f' \in D(2)^\omega$ which differs from f only in a countable number of coordinates, then $X' = \{f' : f \in X\}$ is also HFD. This enables us to get e.g. S -spaces of

cardinality κ if $W(\kappa)$, thus showing that it is consistent to have an S -space of cardinality $2^{\omega_1} = 2^{2^\omega}$. The construction we gave above can also be modified to obtain HFD subgroups of $D(2)^{\omega_1}$ (of size κ), thus yielding e.g. a countably compact, hereditarily normal and hereditarily separable non-Lindelöf topological group (cf. HAJNAL and JUHÁSZ [1976a] for the case $W(\omega_1) = \text{CH}$).

There is also an analogous construction for getting L -spaces of weight κ from $W(\kappa)$, where an L -space is one which is regular, hereditarily Lindelöf but not separable (a dual of S -spaces, cf. HAJNAL and JUHÁSZ [1974]).

Let us note finally, that $(\text{MA} + \neg \text{CH})$ implies that there are no HFD-sets at all. This can be seen e.g. by noting that according to Corollary 1 of Theorem 1.7 $D(2)^{\omega_1}$ is sequentially compact, while of course a convergent sequence can never be dense "in a tail".

Thus, W "works against" $\text{MA} + \neg \text{CH}$ as we have seen with $\Diamond$.

2.7. The next combinatorial principle that we want to illustrate is called $\square_\kappa$, however we shall not need $\square_\kappa$ proper (the interested reader is referred to Chapter B.5) because we only use the following consequence of it that we denote by $E(\kappa)$: There exists a subset $E \subset \kappa$ such that

- (i) $\alpha \in E \rightarrow \text{cf}(\alpha) = \omega$;
- (ii) E is stationary in κ ;
- (iii) for each $\alpha < \kappa$ the set $E \cap \alpha$ is not stationary in α .

$E(\omega_1)$ is a trivially true statement but $E(\omega_2)$ fails in some models of set theory. However Jensen has shown that $V = L$ implies $E(\kappa)$ for "most" regular cardinals κ (cf. DEVLIN [1973]).

An application of $E(\kappa)$ is given in HAJNAL and JUHÁSZ [1976b], where it is shown that the E of $E(\kappa)$ as a space of ordinals has the property that every subspace of E of size less than κ is metrizable, while E is not. Instead of repeating the arguments there we chose to give a more complicated example, which of course has a number of nice additional properties. In order to achieve that however we shall also need a generalized version of $\Diamond$ which reads as follows:

2.8. DEFINITION. Let κ be an uncountable regular cardinal and $E \subset \kappa$ be any stationary set in κ . Then $\Diamond_\kappa(E)$ denotes the statement that there is a sequence $\{S_\alpha : \alpha \in E\}$ such that $S_\alpha \subset \alpha$ and for every $X \subset \kappa$ the set

$$\{\alpha \in E : X \cap \alpha = S_\alpha\}$$

is stationary in κ . Then $\Diamond$ of 2.1 is just $\Diamond_{\omega_1}(\omega_1)$. It is again a result of Jensen

that if $V = L$, then $\diamond_\kappa(E)$ is always true whenever $\kappa > \omega$ is regular and E is stationary in κ (cf. DEVLIN [1973]).

We will actually need the following consequence of $\diamond_\kappa(E)$ that follows easily by means of a “coding” argument:

- There is a sequence $\{\langle S_\alpha, T_\alpha \rangle : \alpha \in E\}$ such that $S_\alpha, T_\alpha \subset \alpha$
 (*) and for any $X, Y \subset \kappa$ the set $\{\alpha \in E : X \cap \alpha = S_\alpha \text{ and } Y \cap \alpha = T_\alpha\}$ is stationary in κ .

Now we can turn to the formulation and proof of the above mentioned result.

2.9. THEOREM. *Suppose E witnesses $E(\kappa)$ and $\diamond_\kappa(E)$ holds. Then there is a topology τ on E which is*

- (i) *locally countable;*
 - (ii) *locally compact, Hausdorff;*
 - (iii) *normal;*
- and for which*
- (iv) *every subspace of E of size less than κ is metrizable, but $\langle E, \tau \rangle$ is not.*

PROOF. To construct the desired topology τ we define topologies τ_α on $E \cap \alpha$ for each $\alpha \in E$ by induction as follows. (Keep in mind that every $\alpha \in E$ is an ω -limit!) Suppose $\alpha \in E$ and that for each $\beta \in E \cap \alpha$ and each $\gamma \in E \cap \beta$ we have already defined a topology τ_β on $E \cap \beta$ and a decreasing sequence of sets $\{V_n(\gamma) : n \in \omega\}$ (this does not depend on β) so that the following conditions are satisfied:

- (1) τ_β is a metrizable topology;
- (2) $\{V_n(\gamma) : n \in \omega\}$ is a neighborhood basis for γ in $\langle E \cap \beta, \tau_\beta \rangle$;
- (3) each $V_n(\gamma)$ is countable, compact and open in $\langle E \cap \beta, \tau_\beta \rangle$;
- (4) the sequence $\gamma_n = \min V_n(\gamma)$ converges to γ in the usual topology of ordinals.

Now, we have two cases to consider. First, if α has no immediate predecessor in E , then we have no new $V_n(\gamma)$ to define and τ_α has to be the topology on $E \cap \alpha$ generated by $\bigcup \{\tau_\beta : \beta < \alpha\}$. Let us note that $\langle E \cap \gamma, \tau_\gamma \rangle$ is always an open subspace of $\langle E \cap \beta, \tau_\beta \rangle$ for $\gamma < \beta < \alpha$, as follows easily from (2), hence of $\langle E \cap \alpha, \tau_\alpha \rangle$ too. Therefore (2), (3) and (4) are automatically valid for α as well, and thus the only thing left to prove is that τ_α is metrizable. To see that, let us put $\alpha^* = \bigcup (E \cap \alpha)$ and choose a closed unbounded subset $C \subset \alpha^*$ with $C \cap E = \emptyset$, which is possible because $E \cap \alpha = E \cap \alpha^*$ is non-stationary in α^* . Then $\alpha^* \setminus C$ can be written as a disjoint union of maximal open intervals:

$$\alpha^* \setminus C = \bigcup \{(\alpha_i, \beta_i) : i \in I\},$$

where $\alpha_i, \beta_i \in C$. We claim that for each $i \in I$ the set $(\alpha_i, \beta_i) \cap E$ is open in $\langle E \cap \alpha, \tau_\alpha \rangle$. Indeed, if $\gamma \in E \cap (\alpha_i, \beta_i)$ then by (4) there is $n \in \omega$ for which $V_n(\gamma) \subset (\alpha_i, \gamma] \subset (\alpha_i, \beta_i)$. But then $\langle E \cap \alpha, \tau_\alpha \rangle$ is the topological sum of its subspaces $E \cap (\alpha_i, \beta_i)$, which are metrizable by (1), hence so is τ_α .

Next assume that β is the immediate predecessor of α in E . Then we first have to define the sets $V_n(\beta)$ which will form a neighborhood basis of β in $\langle E \cap \alpha, \tau_\alpha \rangle$. (Note that $E \cap \alpha = (E \cap \beta) \cup \{\beta\}$.) To this end we again have to distinguish two cases.

Case a. $\bigcup (E \cap \beta) = \beta$ and S_β and T_β are disjoint unbounded subsets of $E \cap \beta$. Then we choose two sequences $A = \{\sigma_n : n \in \omega\} \subset S_\beta$ and $B = \{\rho_n : n \in \omega\} \subset T_\beta$ such that $\sigma_n \nearrow \beta$ and $\rho_n \nearrow \beta$. Clearly then A and B are closed discrete subsets of the (metrizable) space $\langle E \cap \beta, \tau_\beta \rangle$, hence we can put pairwise disjoint neighborhoods about the points of $A \cup B$, say $V_{k_n}(\sigma_n)$ and $V_{l_n}(\rho_n)$, where we can also assume, by (4), that

$$\sigma_{n-1} < \min V_{k_n}(\sigma_n) \quad \text{and} \quad \rho_{n-1} < \min V_{l_n}(\rho_n)$$

for each $n \in \omega \setminus \{0\}$.

Now we can define the neighborhoods $V_m(\beta)$ by putting

$$V_m(\beta) = \bigcup \{V_{k_n}(\sigma_n) \cup V_{l_n}(\rho_n) : n \in \omega \setminus m\} \cup \{\beta\}.$$

Clearly $V_m(\beta)$ is then countable and $V_m(\beta) \cap (E \cap \beta)$ is open in τ_β , hence we indeed get a topology τ_α on $E \cap \alpha = (E \cap \beta) \cup \{\beta\}$ taking the $V_m(\beta)$ as an open neighborhood basis of β . That each $V_m(\beta)$ is also compact in τ_α is proved easily from the inductive hypotheses, just like in the proof of 2.2. Moreover $\beta_m = \min V_m(\beta) \geq \min\{\sigma_{m-1}, \rho_{m-1}\}$ for each $m > 0$, hence $\beta_m \rightarrow \beta$, showing that (2)–(4) are satisfied for α . Finally the metrizability of τ_α follows from the fact that it is first countable and regular (being locally compact and Hausdorff) and throwing away a single point from $E \cap \alpha$, namely β , we get a metrizable subspace, namely $\langle E \cap \beta, \tau_\beta \rangle$ (cf. HAJNAL and JUHÁSZ [1976b]).

Case b is when case a does not hold. Then we simply add β as an isolated point to get τ_α , and put $V_n(\beta) = \{\beta\}$ for each $n \in \omega$. It is trivial then that conditions (1)–(4) will be satisfied.

Thus we can define τ_α for each $\alpha \in E$ and then put $\bigcup \{\tau_\alpha : \alpha \in E\}$ as a basis for the topology τ on E . Clearly then (i) and (ii) hold, moreover every subspace of $\langle E, \tau \rangle$ of cardinality less than κ is a subspace of some $\langle E \cap \alpha, \tau_\alpha \rangle$ and hence is metrizable.

To see that $\langle E, \tau \rangle$ is normal, let H and K be any two disjoint closed sets

in it. If both are bounded, they are both contained in an open metrizable subspace $\langle E \cap \alpha, \tau_\alpha \rangle$ hence can be separated, trivially. They cannot both be unbounded though, because suppose they were, then the set

$$H' \cap K' \cap \{\beta \in E: H \cap \beta = S_\beta \text{ and } K \cap \beta = T_\beta\}$$

would be non-empty by (*) (here of course H' and K' denote the sets of all ordinary limit points of H and K , respectively), and by our construction any such β is in the τ -closure of both H and K . So we can assume e.g. that H is bounded and K is not. Now let $\nu \in \kappa$ be an ω_1 -limit such that $H \subset \nu$. If α is the smallest member of $E \setminus \nu$, then $\nu < \alpha$, moreover $E \cap \nu = E \cap \alpha \supset H$. Then H and $K \cap \alpha$ are disjoint closed sets in $\langle E \cap \alpha, \tau_\alpha \rangle$, hence can be separated by τ_α -open, hence τ -open, sets U and V . On the other hand, for each $\beta \in K \setminus \alpha$ we have $\nu < \beta$, hence we can choose k_β such that $V_{k_\beta}(\beta) \subset E \setminus \nu$, and then the open sets U and

$$V \cup \bigcup \{V_{k_\beta}(\beta): \beta \in K \setminus \alpha\}$$

clearly separate H and K , hence we have (iii).

Finally, we claim that $J = \{\alpha \in E: \alpha \text{ is not isolated in } \langle E, \tau \rangle\}$ is a stationary subset of κ . Indeed, by our construction, for any two disjoint and unbounded subsets S and T of E we have

$$J \supset S' \cap T' \cap \{\alpha \in E: S \cap \alpha = S_\alpha \text{ and } T \cap \alpha = T_\alpha\},$$

so J contains a set which is stationary by (*). Knowing this about J we show that $\langle E, \tau \rangle$ is not even metacompact, hence is not metrizable. Indeed, the family $\{E \cap (\alpha + 1): \alpha \in E\}$ is an open cover of $\langle E, \tau \rangle$ and if $\mathcal{G}$ is any open refinement of it then for each $\alpha \in J$ there is $n \in \omega$ with $V_n(\alpha) \subset G_\alpha$ for some $G_\alpha \in \mathcal{G}$. Then $f(\alpha) = \min V_n(\alpha) < \alpha$, hence f is a regressive function on J (cf. Theorem 2.3 of Chapter B.3) so by Neumer's theorem there is $S \subset J$, $|S| = \kappa$ and $\beta \in E$ such that $f(\alpha) = \beta$ for all $\alpha \in S$. But clearly each G_α is bounded in κ , hence

$$|\{G_\alpha: \alpha \in S\}| = \kappa,$$

and also

$$\beta \in \bigcap \{G_\alpha: \alpha \in S\} \neq \emptyset$$

so $\mathcal{G}$ is not point-finite. Thus (iv) is also satisfied and the proof is completed. $\square$

Finally we are going to look at some applications of Kurepa trees. Let us recall (cf. Chapter B.4) that a tree of height ω_1 is called a Kurepa tree if it has countable levels and more than ω_1 branches. Thus e.g. for any $\kappa > \omega_1$

the tree $T \setminus T_{\omega_1}$ of $W(\kappa)$ is always a Kurepa tree. It is shown in Chapter B.4 that the existence of Kurepa trees is both consistent with and independent of the usual axioms of set theory.

The first application, due to K. Kunen, is concerned with the following situation. Suppose we have CH, i.e. $2^\omega = \omega_1$, but $2^{\omega_1} > \omega_2$. Now it is well known that a compact space of countable weight is either countable or has cardinality 2^ω , independently of CH. Is it true then that in the above situation the cardinality of a compact space of weight $\leq \omega_1$ is either $\leq \omega_1$ or equal to 2^{ω_1} ? It turns out that the answer to this question can be both "yes" and "no", depending on your set theory. We shall illustrate one of these answers by proving the following theorem.

2.10. THEOREM. *Suppose $2^\omega = \omega_1$, $2^{\omega_1} > \omega_2$, and T is a Kurepa tree with exactly ω_2 branches. Then there is a compact space of weight ω_1 and of cardinality ω_2 .*

PROOF. We claim that the subspace X of $D(2)^T$ consisting of the characteristic functions of all connected chains of T is as required. (By a connected chain we mean a chain C such that $t \in C$ and $s < t$ implies $s \in C$ as well.) Since *not* being a connected chain is clearly always decided by two members of T , the complement of X in 2^T is open, hence X is compact. $|X| = \omega_2$ holds because there are only ω_1 bounded connected chains in T by CH, and there are exactly ω_2 unbounded ones, by assumption. Finally, $w(X) = \omega_1$ is trivial from $w(D(2)^T) = |T| = \omega_1$. $\square$

Our last result answers a question raised by R. Sikorski in 1950, namely, does there exist a Lindelöf ω_1 -metrizable space of cardinality $> \omega_1$ (cf. SIKORSKI [1950], p. 132)]. W. Weiss and the present author have recently shown that the complete answer to this (really very natural) question is given by a strange tree.

2.11. THEOREM. *There exists a Lindelöf ω_1 -metrizable space of cardinality $> \omega_1$ if and only if there is a Kurepa tree with no Aronszajn subtree.*

We shall not give the proof of this result here, it will appear in JUHÁSZ and WEISS [1977]. We only mention that $V = L$ implies the existence of such trees, as was shown by R. Jensen (cf. DEVLIN [1974]), while of course it is consistent that there are no Kurepa trees at all (cf. Chapter B.4).

References

- AARTS, J.M. and LUTZER, D.J.
 [1974] Completeness properties designed for recognizing Baire spaces, *Dissertationes Math.*, **116**.
- DEVLIN, K.J.
 [1973] *Aspects of Constructibility*, Lecture Notes in Mathematics, Vol. 354 (Springer, Berlin).
 [1974] Order types, trees, and a problem of Erdős and Hajnal, *Period. Math. Hungar.*, **5**, 153–160.
- HAJNAL, A. and JUHÁSZ, I.
 [1971] A consequence of Martin's axiom, *Indag. Math.*, **33**, 457–463.
 [1974] On hereditarily α -Lindelöf and α -separable spaces, II, *Fund. Math.*, **81**, 147–158.
 [1976a] A separable normal topological group need not be Lindelöf, *General Topology and Appl.* **6**, 199–205.
 [1976b] On spaces in which every small subspace is metrizable, *Bull. Acad. Polon. Sci.*
- HECHLER, S.
 [1976] On some weakly compact spaces and their products, *General Topology and Appl.*
- JUHÁSZ, I.
 [1971] Cardinal functions in topology, Mathematical Centre Tract, Vol. 34 (Math. Centre, Amsterdam).
- JUHÁSZ, I. and WEISS, W.
 [1977] On a problem of Sikorski. *Fund. Math.*
- JUHÁSZ, I., KUNEN, K. and RUDIN, M.E.
 [1977] Two more hereditarily separable non-Lindelöf spaces, *Canad. J. Math.*
- KUNEN, K. and TALL, F.D.
 [1977] Between MA and SH.
- MARTIN, D.A. and SOLOVAY, R.
 [1970] Internal Cohen extensions, *Ann. Math. Logic*, **2**, 143–178.
- MALYHIN, V.I. and ŠAPIROVSKII, B.E.
 [1973] Martin's axiom and properties of topological spaces, *Dokl. Akad. Nauk SSSR*, **213**, 532–535.
- OSTASZEWSKI, A.J.
 [1975] On countably compact, perfectly normal spaces, *J. London Math. Soc.*
- RUDIN, M.E.
 [1955] Countable paracompactness and Souslin's problem, *Canad. J. Math.*, **7**, 543–547.
 [1975] Lectures on set theoretic topology, CBMS Regional Conference Series in Mathematics, Vol. 23.
- ŠAPIROVSKII, B.E.
 [1972] On separability and metrizability of spaces with Suslin's condition, *Soviet Mat. Dokl.*, **13**, 1633–1638.
- SIKORSKI, R.
 [1950] Remarks on some topological spaces of high power, *Fund. Math.*, **37**, 125–136.
- STEPHENSON, R.M.
 [1972] Discrete subsets of perfectly normal spaces, *Proc. Am. Math. Soc.*, **34**, 605–608.
- TALL, F.D.
 [1974] The countable chain condition vs. separability, *General Topology and Appl.*, **4**, 315–339.

PART C

Recursion Theory

Guide to Part C: *Recursion Theory*

with the cooperation of
Y.N. MOSCHOVAKIS

C.1. ENDERTON	
<i>Elements of recursion theory</i>	527
C.2. DAVIS	
<i>Unsolvable problems</i>	567
C.3. RABIN	
<i>Decidable theories</i>	595
C.4. SIMPSON	
<i>Degrees of unsolvability: a survey of results</i>	631
C.5. SHORE	
<i>α-recursion theory</i>	653
C.6. KECHRIS and MOSCHOVAKIS	
<i>Recursion in higher types</i>	681
C.7. ACZEL	
<i>An introduction to inductive definitions</i>	739
C.8. MARTIN	
<i>Descriptive set theory: projective sets</i>	783

Strictly speaking, recursion theory is the study of the class of recursive, or effectively computable, functions and their applications to mathematics. A broader interpretation is when recursion theory is taken to mean the study of the general process of definition by recursion, not just on natural numbers but on all types of mathematical structures. The first four chapters of this Part fit under the narrow definition, the last four under the broader one.

The class of recursive functions is defined and studied in Enderton's introductory chapter. This chapter discusses the arguments for the identification of this class with the "effectively calculable" functions (Church's Thesis). It also introduces the reader to many of the ways that the basic notions can be applied.

The next three chapters take up in depth topics introduced in Enderton's chapter. Martin Davis's chapter pursues the uses of the theory of recursive functions for showing that certain classes of problems cannot be effectively decided — the word problem for groups being one of the best known. The related problem of decidable versus undecidable theories of first-order logic is discussed in Rabin's chapter.

Among undecidable problems, some are more undecidable than others. The definition of "degree" of unsolvability is introduced in Section 8 of Enderton's paper and a survey of important results on these degrees is given in Simpson's chapter.

Moving to the broader definition of recursion theory we come to Shore's chapter on the generalization of recursion theory to admissible ordinals. Shore presents a fine introduction to the basic notions and, as a case study, shows what new considerations arise when the Splitting Theorem is generalized to admissible ordinals. The chapter also contains a very useful annotated bibliography to the study of α -recursion theory.

The study of Kleene recursion in higher types (recursive functions of functions of functions, say, rather than recursive functions of natural numbers) has always been more or less inaccessible to all but the dedicated specialist — due to the difficulty of the basic papers in the subject. This situation should be remedied in the chapter by Kechris and Moschovakis, where a conceptually simple approach via inductive definability is taken.

The study of inductive definitions in general is taken up in Aczel's chapter. It should interest logicians of all persuasions since it combines the concerns of the recursion-theorist with the vantage points of the model-theorist and proof-theorist.

Martin's chapter discusses one of the major applications of recursion theory — to descriptive set theory. Here definability considerations over the continuum give rise to a beautiful theory which finds its origins in the French "constructivist" school of Borel, Baire and Lebesgue.

We had planned to have a chapter on the more "practical" aspects of recursion theory, those where running times of programs and computational complexity appear, but this chapter did not materialize. Among other chapters of the *Handbook* relevant to recursion theory we mention Statman's chapter on the equation calculus (in Part D), and Makkai's chapter on admissible sets (in Part A). The recursion-theorist might also be interested to see some proof-theoretic applications of recursion theory in Feferman's chapter in Part D.

Elements of Recursion Theory

HERBERT B. ENDERTON

Contents

Introduction	528
1. Informal computability	528
2. Turing machines	530
3. Church's thesis	533
4. Universal machines and normal form	535
5. Oracles and functionals	539
6. Recursive enumerability	541
7. Logic and recursion theory	546
8. Degrees of unsolvability	549
9. Creative and lesser sets	552
10. Definability and recursion	554
11. Recursive analogues of classical objects	560
References	564

Introduction

This chapter presents an expository treatment of the elements of recursive function theory. It makes no claims of advancing to the frontiers of research in this field. It does attempt to indicate what background would be required of someone heading that way.

The proofs in this chapter are often merely sketched, with indication of the main ideas involved. There are several books that give more thorough treatment to these topics. The primary reference in this field is ROGERS [1967]. A more condensed treatment can be found in Chapters 6 and 7 of SHOENFIELD [1967]. Turing machines are discussed, among other places, in books by YASUHARA [1971] and by DAVIS [1958]. There is a fairly recent book on degrees of unsolvability by SHOENFIELD [1971] and an older one by SACKS [1963]. Finally, the classic book by KLEENE [1952] contains much recursion theory.

1. Informal computability

The simplest conception of recursive functions is as “effectively computable” functions. We will consider initially functions from natural numbers to natural numbers, postponing the matter of functions on other sets. Let $\mathbb{N}$ be the set $\{0, 1, 2, \dots\}$ of natural numbers, and let $\mathbb{N}^k$ be the cartesian product $\mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N}$ with k factors. Then the objects we want to consider will be functions f with $\text{dom } f \subseteq \mathbb{N}^k$ for some positive k and $\text{ran } f \subseteq \mathbb{N}$. Such an object will be called a k -place partial function. The word “partial” is a reminder that the domain is only a subset, possibly proper, of $\mathbb{N}^k$. (The partial function is said to be *total* if its domain is all of $\mathbb{N}^k$.)

It is clear from cardinality considerations that there are $2^{\aleph_0}$ k -place partial functions for each positive k . From this huge inventory we want to select the $\aleph_0$ functions that are recursive. We begin in this section with an intuitive description of the notions we seek to capture. And then in the next section we will turn to the methods for making the ideas precise.

Call a k -place partial function f *effectively computable* when there exists an effective procedure (i.e., an algorithm) that calculates f correctly. Now an effective procedure must meet the following criteria.

(i) There must be exact instructions (i.e., a program), finite in length, for the procedure. These instructions cannot demand any cleverness or even understanding on the part of the person or machine following them.

Executing the instructions must be a matter of merely following directions carefully.

(ii) If the procedure is given a k -tuple $\mathbf{x}$ in $\text{dom } f$, then after a finite number of discrete steps the calculation must terminate and produce $f(\mathbf{x})$.

(iii) If the procedure is given a k -tuple $\mathbf{x}$ that does not belong to $\text{dom } f$, then the procedure might go on forever, never halting. Or it might get stuck at some point, but it must not pretend to produce a value for f at $\mathbf{x}$.

One can picture an industrious and diligent clerk, well supplied with scratch paper, tirelessly following his instructions. Alternatively, one can picture an automated version, a digital computer executing a program.

Despite the fact that we have given only a suggestive description and not a mathematical definition, it is possible to develop nearly all of the theory of recursive functions on just this informal basis. (The recursive functions are the effectively computable functions, but we reserve the term "recursive" for the mathematically defined concept.) For evidence of this possibility, we refer the reader to the book ROGERS [1967].

As examples of effectively computable functions we can cite addition and multiplication of natural numbers. Effective procedures for these functions (using decimal representation) are taught in the elementary schools. Any function with a finite domain is effectively computable. The instructions for computing such a function can contain a table listing all of its values.

There are several sorts of restrictions of a practical nature that we do *not* impose on effective procedures.

(i) Although each argument given the procedure as input must be a (finite) natural number, there is no bound imposed in advance on the size of the arguments. We do not rule out arguments that exceed the number of electrons in the universe, for example.

(ii) Although the procedure must produce $f(\mathbf{x})$, when $\mathbf{x} \in \text{dom } f$, after a finite number of steps, there is no bound imposed in advance on this number.

(iii) Similarly, there is no bound imposed in advance on the amount of scratch paper (memory space) the procedure might require. Even multiplication of very large numbers can require large amounts of scratch paper.

These considerations are relevant to the comparison of effective computability to "practical computability". A person with a digital computing machine may regard a function f as being computable only when $f(\mathbf{x})$ is computable on his machine in a reasonable length of time. Of course, the matter of what is reasonable may change from day to day. And next year he hopes to get a faster machine with more memory space and tape drives.

At that time, his idea of what is computable in a practical sense will be extended considerably.

The class of effectively computable functions is obtained in the ideal case where all of the practical restrictions on running time and memory space are removed. Thus the class is a theoretical upper bound on what can ever in any century be considered computable.

It should be clear that if f and g are functions that agree at all but finitely many arguments, then f is effectively computable iff g is also effectively computable. Thus the question whether a function is effectively computable hinges solely on the behavior of that function in neighborhoods of infinity.

2. Turing machines

There are many equivalent ways of formulating the definition of recursiveness. A version phrased in terms of imaginary computing machines was given by the English mathematician Alan Turing in a fundamental paper (TURING [1936]). (Related work was done simultaneously but independently by Emil Post in New York; see POST [1936].) Turing had the disadvantage of formulating this definition prior to the development of actual digital computers. In fact the flow of information was from the abstract to the concrete: von Neumann was familiar with Turing's work, and Turing himself later played an enthusiastic role in the development of computers.

On an informal level, we can begin by picturing a Turing machine as a black box together with a tape. The tape is marked off into squares, and each square can contain either the blank symbol 0 or the non-blank symbol 1. The tape is potentially infinite in both directions, in that we never come to the end of it, but at any time only finitely many squares can be non-blank. Initially the tape contains the input numbers, and ultimately it contains the output number. At intermediate times it serves as memory space for the calculation.

If we open up the black box, we find that it is a very simple device. It is capable of examining only one square of the tape at a time. The device contains a finite list of instructions (or *states*) $q_0, q_1, \dots, q_n$. Each instruction can indicate two possible courses of action, one to be followed if the tape square under scrutiny contains a 0, the other to be followed if it contains a 1. In either event, a course of action can only consist of the following three steps:

(i) A symbol (possibly the same as the old symbol) is written on the tape square being scanned, thereby erasing the previous symbol.

(ii) The tape is moved one square right or left.

(iii) The next instruction is specified.

Thus the list of instructions determines a transition function that, given the number of the present instruction and the symbol being scanned, produces the three-part course of action. We can formalize these ideas by taking the Turing machine simply to be this transition function.

2.1. DEFINITION. A *Turing machine* is a function M such that for some natural number n ,

$$\text{dom } M \subseteq \{0, 1, \dots, n\} \times \{0, 1\},$$

$$\text{ran } M \subseteq \{0, 1\} \times \{L, R\} \times \{0, 1, \dots, n\}.$$

For example we might have $M(3, 1) = (0, L, 2)$. The intended meaning of this is that whenever the machine comes to instruction q_3 while scanning a square in which 1 is written, it is to erase the 1 (leaving a 0 in the square), move the tape so as to examine the square just to the left of the present square, and proceed next to instruction q_2 . If $M(3, 1)$ is undefined, then whenever the machine comes to instruction q_3 while scanning a square in which 1 is written, it halts. (This is the only way of stopping a calculation.)

This intended interpretation is not embodied in the formal definition of a Turing machine. But it does motivate and guide the formulation of all subsequent definitions. In particular, we can define what it means for a machine M to move (in one step) from one configuration to another. We do not need to present the formal definitions here, since they are only translations of our informal ideas.

The input/output format consists of strings of 1's, separated by 0's. Let $\lceil x \rceil$ be a string of 1's of length $x + 1$. Thus

$$\lceil x_1 \rceil 0 \lceil x_2 \rceil 0 \cdots 0 \lceil x_k \rceil$$

is the result of combining k strings of 1's, each separated from the next by a 0.

At last we can define recursiveness. A k -place partial function f is said to be *recursive* if there exists a Turing machine M such that whenever we start M at instruction q_0 scanning the leftmost symbol of

$$\lceil x_1 \rceil 0 \lceil x_2 \rceil 0 \cdots 0 \lceil x_k \rceil$$

(with the rest of the tape blank), then:

(i) If $f(x_1, \dots, x_k)$ is defined, then M eventually halts scanning the leftmost symbol of

$$\lceil f(x_1, \dots, x_k) \rceil$$

and with the tape blank to the right of this string.

(ii) If $f(x_1, \dots, x_k)$ is undefined, then M never halts.

If R is a k -ary relation on the natural numbers, then R is said to be *recursive* if its characteristic function $\chi_R : \mathbb{N}^k \rightarrow \{0, 1\}$ is recursive. (Caution: If a k -place partial function is recursive, then it does not follow that its graph is a recursive $(k + 1)$ -ary relation.)

For example the identity function $f(x) = x$ is recursive, being computed by the empty machine. A less trivial case is addition $x + y$, which is computed by the machine whose values are listed in Table 1. The comments to the right are to help the reader, not the machine. (Turing defined M to be a set of quintuples instead of a function from pairs to triples. The table, being the graph of M , is essentially a set of quintuples.)

Table 1

0 1	1 R 0	pass over x
0 0	1 R 1	fill gap
1 1	1 R 1	pass over y
1 0	0 L 2	end of y
2 1	0 L 3	erase a 1
3 1	0 L 4	erase another 1
4 1	1 L 4	back up
4 0	0 R 5	halt

It is an exercise in programming to produce Turing machines for multiplication and exponentiation.

We should remark that many of the details of our definition of a Turing machine are somewhat arbitrary. If there were more than one tape, the class of computable functions would remain unchanged (although some functions could be computed more rapidly). Similarly we could allow more than the symbols 0 and 1. Or we could have the tape extend in only one direction from a starting point, instead of both directions. None of this affects the class of computable functions. What is essential in the definition is the provision for arbitrarily large amounts "scratch-pad" storage space and arbitrarily long calculations.

We can give a specific example of a non-recursive function by using the "busy beaver competition" of RADO [1962]. An n -state entry in this competition is a Turing machine M with $n + 1$ instructions $q_0, \dots, q_n$, the last of which is used only for halting (both $M(n, 0)$ and $M(n, 1)$ are undefined), and such that when started on a blank tape, M eventually halts. When M does halt, its score in the competition is the number of 1's on the tape. Thus the machine tries to write as many 1's on the tape as it possibly can, but it must halt. Let $\Sigma(n)$ be the maximum possible score for an n -state entry.

2.2. THEOREM (RADO [1962]). *The function Σ is not recursive. In fact for any total recursive f on $\mathbb{N}$, we have $f(x) < \Sigma(x)$ for all sufficiently large x .*

PROOF. The function whose value at x is

$$\max[f(2x + 2), f(2x + 3)]$$

is recursive, and hence is computed by some machine M having, say, k instructions. For each x , consider a machine N_x that writes '1' on a blank tape and then behaves like M . Then N_x is a $(x + k + 2)$ -state entry in the busy beaver competition. So its score (the number displayed above plus 1) is bounded by $\Sigma(x + k + 2)$, which for all $x \geq k$ is bounded by $\Sigma(2x + 2)$. $\square$

We will construct other non-recursive functions later, but the Σ function has a striking simplicity. The first few values of Σ are known: $\Sigma(1) = 1$, $\Sigma(2) = 4$, and $\Sigma(3) = 6$ (LIN and RADO [1965]). Next $\Sigma(4) = 13$ (BRADY [1966, 1975]). Beyond this point, only lower bounds are known. $\Sigma(5) \geq 17$, $\Sigma(6) \geq 35$, $\Sigma(7) \geq 22961$, and $\Sigma(8) > 8 \times 10^{44}$ (GREEN [1964]).

3. Church's thesis

In Section 1 we discussed an informal concept of computability. In Section 2 we defined the mathematical concept of recursiveness. Do these two match? That is, is the concept of recursiveness the correct formalization of our intuitive concept of effective computability? The claim that it is indeed correct is known as Church's thesis. This claim was advanced and defended by CHURCH [1935, 1936], and has been almost universally accepted.

There are two arguments supporting the view that the class of recursive functions is broad enough to contain all effectively computable functions.

The first has to do with specific procedures: the procedures that have been felt to be effective have, when examined, been found to be executable by Turing machines. The second argument has to do with the class of effective procedures as a whole: the several attempts that were made to formalize the concept of computability have all yielded concepts equivalent to recursiveness. In particular, the natural ways of liberalizing the definition of recursiveness (such as allowing several tapes) in the end yield notions equivalent to recursiveness. (The proofs of these results are, for the most part, not difficult once the techniques of the following section are known).

Historically, the first appearance of a definition of recursiveness was in Kurt Gödel's original paper (GÖDEL [1931]) on the incompleteness of formal systems. He defined a relation to be *entscheidungsdefinit* if it was binumerable in a certain formal system of number theory. (The concept of binumeration may be found in Chapter D.1.) This is equivalent to our definition of recursive relation. But Gödel was not at this time attempting to formalize the concept of effective decidability or computability, and attention was not focussed on this definition. In the same paper he defined a class of functions called "recursive" (*rekursiv*); this is now called the class of primitive recursive functions. The name "recursive" was appropriate, since the central feature of the definition was a provision for finding $f(n+1)$ from $f(n)$.

Gödel visited Princeton several times in the 1930's, before moving there permanently in 1940. In 1934, during one of these visits, he gave a talk for which mimeographed notes were circulated. The notes were taken by Kleene and Rosser, who about this time completed dissertations at Princeton under Church. (The notes were eventually published as GÖDEL [1965].) In this talk he raised the issue of effective computability. He noted that more general forms of recursion would have to be admitted before his previous recursive functions could include all computable functions. He then defined a class he called "general recursive functions", using ideas that had been suggested to him in a letter from Herbrand. (This definition, which involved formal rules for deriving equations from others, is also equivalent to our definition of recursiveness.)

Church had been at Princeton since 1929 and together with his student Kleene had developed the concept of λ -definable functions. The question of the relationship between λ -definability and effective computability was studied by Church. CHURCH [1936] not only contained the proposal now bearing his name, but also provided the first example of an unsolvable decision problem. This is the problem whether a formula in the λ -calculus has a normal form, which can be regarded as a decision problem in

elementary number theory. The proof of the equivalence of the concept of λ -definable functions and the concept of general recursive functions was due primarily to KLEENE [1936b].

TURING [1936] referred to Church's paper, and presented yet another definition of recursiveness (essentially the definition of Section 2). Turing had independently had the idea of formalizing the concept of effective computability, but was led to publish only when Church's paper appeared. In an appendix, Turing proved the equivalence of his definition to λ -definability.

POST [1936] described Church's thesis as being not a definition or an axiom but a natural law, a "fundamental discovery" concerning "the mathematicizing power of Homo Sapiens", in need of "continual verification".

Until now we have dealt with functions as the basic objects of study; we have made scant reference to k -ary relations on $\mathbb{N}$. Actually recursion theory can be developed in terms of either functions or relations, and with interchangeable results. We can, informally, call a relation R *decidable* if there is an effective procedure that, given any x , replies "yes" if $x \in R$ and replies "no" if $x \notin R$. (In discussing relations, we will write $x \in R$ and $R(x)$ synonymously.) Then R is decidable iff the characteristic function of R is effectively computable. Thus a consequence of Church's thesis (equivalent in fact to the original form) is that the concept of a recursive relation is the correct formalization of the informal concept of a decidable relation.

4. Universal machines and normal form

The initial application of recursive functions was to prove incompleteness theorems of logic. For that purpose, no deep results on the internal structure of the class of recursive functions are required. And in fact a more restricted class, such as the primitive recursive functions mentioned in the preceding section, would suffice.

But as will be seen, there are other applications for recursive functions. And if for no other reason, the recursive functions would be studied for their own interest as the effectively computable functions. And the basic fact that gets such a study off the ground is the possibility of encoding machines into integers that can then be supplied as input to other (or the same) machines.

There is a direct analogy here with actual digital computers. The earliest

such computers were programmed by setting switches and inserting wires into plugboards. It was then realized (by von Neumann) that for a suitably constructed computer, the program could be coded into machine words (i.e., integers) and stored in the machine in the same manner as data — the stored-program computer. The first practical benefit of this approach to programs is the speed at which new programs can be loaded into the computer to replace old programs. But a more significant benefit (for our purposes) is the possibility of executive programs, e.g. operating systems. An executive program accepts another program as incoming data. The executive program might then study the incoming object program and see that its instructions are carried out.

The ideas behind stored-program computers can be carried over to Turing machines. (Historically it was the other way around.) A Turing machine M might be given two numbers as input, one of them a suitable encoding of Turing machine N , and the other a number x . Machine M might then serve as an executive program, and the output might be just the result of applying N to x . M can then be called a *universal* Turing machine.

Carrying out these ideas and constructing a universal Turing machine turns out to be a straightforward (if somewhat lengthy) procedure. We will outline how it goes. First of all, each Turing machine is a finite object, and so can be encoded as a natural number under some fixed encoding. We can, for example, define the encoding

$$\langle x_0, x_1, \dots, x_n \rangle = 2^{x_0+1} 3^{x_1+1} \dots p_n^{x_n+1}$$

in powers of primes as a way of condensing a finite string of numbers to a single number. We then need a decoding function $(x)_i$, with the property that for $i \leq n$,

$$(\langle x_0, x_1, \dots, x_n \rangle)_i = x_i.$$

Turing machines can be found to effect the above encoding, and inversely to do the decoding.

At any point in the history of a Turing machine calculation, the entire configuration of the machine (the tape contents, the instruction number, and the square being scanned) can be described by a finite amount of information, and so can again be encoded into a number, called an *instantaneous description*. Then a *computation record* for machine M is a number encoding a finite sequence of instantaneous descriptions meeting the following conditions.

(i) The first instantaneous description specifies instruction q_0 (the “initial state”).

(ii) The last one has the machine at an instruction q_i and scanning a symbol s for which $M(i, s)$ is undefined (a "halting configuration").

(iii) Each one is related to the next in that M , when in the configuration given by one instantaneous description, moves in one step to the configuration given by the next.

Thus a computation record is a natural number that encodes the entire history of one calculation by M , from its initial state q_0 (presumably with some input of interest on the tape) until it halts.

All this encoding would be pointless were it not for the fact: the results of the encoding are *recursive* functions and relations. That is, in going through the details of this encoding, one can verify at every step that Turing machines exist to handle the concepts involved. In the end one has the following two results.

(i) There is a recursive ternary relation T that holds of $e, \langle x_1, \dots, x_k \rangle$, and y iff e encodes a Turing machine and y is a computation record for that machine, starting with $\lceil x_1 \rceil 0 \lceil x_2 \rceil 0 \dots 0 \lceil x_k \rceil$ on the tape.

(ii) There is a recursive function U such that whenever $T(e, \langle x_1, \dots, x_k \rangle, y)$ holds, then $U(y)$ — the upshot of y — is the output value of the calculation (provided the halting configuration is such that this makes sense).

Even without the details, it should appear that T is intuitively decidable and U is computable. And so one would expect them to be recursive; that expectation is correct. Next we define, for each k , the k -place partial function

$$\{e\}^k(x_1, \dots, x_k) = U[\text{the least } y \text{ such that } T(e, \langle x_1, \dots, x_k \rangle, y)].$$

Here we write "the least y " although it is quite possible that no such y exists; if there is no such y then the function is undefined at that point. We abbreviate all this by the letter μ :

$$\{e\}^k(x_1, \dots, x_k) = U(\mu y T(e, \langle x_1, \dots, x_k \rangle, y)).$$

(The notation $\{e\}^k$ is Kleene's; the notation $\varphi_e^{(k)}$ is used by Rogers. The superscript k is omitted whenever possible.)

We can now conclude the following fundamental theorem. The theorem in this form is due to KLEENE [1936a, 1943], but universal Turing machines appeared in the original paper by TURING [1936].

4.1. Normal Form Theorem

(i) *The $(k+1)$ -place partial function whose value at $(e, x_1, \dots, x_k)$ is $\{e\}^k(x_1, \dots, x_k)$ is recursive.*

- (ii) For each e , the k -place partial function $\{e\}^k$ is recursive.
- (iii) Every k -place recursive partial function equals $\{e\}^k$ for some e .

The number e will be called an *index* of $\{e\}^k$. Thus a partial function is recursive iff it has an index.

We want next to use this work to prove the unsolvability of the halting problem. Suppose we give input x to machine M and start it running. After the first million steps, we might become suspicious that it will never halt. On the other hand, maybe if we have just a little more patience, it will halt after a few more steps. Is there any way to test which of these two situations we are in? No, there is not. There is no effective procedure that, given M and x , will decide whether or not this calculation ever terminates. This is the content of the theorem below. For a partial function f , we write $f(x) < \infty$ to mean that $f(x)$ is defined.

4.2. THEOREM (unsolvability of the halting problem). *Neither $\{(x, y): \{x\}(y) < \infty\}$ nor $\{x: \{x\}(x) < \infty\}$ is recursive.*

PROOF. Our description of this proof (and others) relies on the reader's informal ideas of effective computability, but it can be translated into a rigorous description involving Turing machines.

Let $K = \{x: \{x\}(x) < \infty\}$. It suffices to show that K , the diagonal of the halting problem, is not recursive. We use a classical diagonal argument. Consider the function

$$g(x) = \begin{cases} \{x\}(x) + 1 & \text{if } x \in K, \\ 0 & \text{if } x \notin K. \end{cases}$$

The function g is total, but it cannot be recursive (because $g(e) \neq \{e\}(e)$ for each e). But if K were recursive, then g would be. So K is not recursive. $\square$

In the foregoing sections, we have been totally indifferent to questions regarding just how long it took a Turing machine to compute a function value. But now suppose we examine $\Phi_e(x)$, the number of steps the machine with index e uses in computing $\{e\}(x)$. For any recursive function, we have the choice of infinitely many different machines to compute it. Some recursive functions are so stubborn that any available machine takes almost forever:

4.3. THEOREM (RABIN [1960]). *For any total recursive H on $\mathbb{N}$, we can find a total recursive $F : \mathbb{N} \rightarrow \{0, 1\}$ such that for any index e of F ,*

$$\Phi_e(x) > H(x)$$

for all sufficiently large x .

The proof involves gradually detecting indices of fast machines, and defining F so as to disagree somewhere with the result of such machines.

A stronger result is the speed-up theorem, which indicates that a function need not have any fastest index, or even any almost fastest index for any reasonable meaning of "almost".

4.4. SPEED-UP THEOREM (BLUM [1967]). *For any total recursive function G on $\mathbb{N} \times \mathbb{N}$, we can find a total recursive $F : \mathbb{N} \rightarrow \{0, 1\}$ such for each index i of F there exists another index j of F such that*

$$G(x, \Phi_j(x)) < \Phi_i(x)$$

for all sufficiently large x .

For example, take $G(x, y) = 2^y$. Then for any machine computing F , there exists another machine exponentially faster for almost all inputs. The theorems of Rabin and Blum are actually more general than we have indicated. In these theorems $\Phi_e(x)$ can be any reasonable measure of the complexity of computing $\{e\}(x)$, subject only to some very modest assumptions.

For any total recursive function L on $\mathbb{N}$ we can define the complexity class C_L of functions almost always computable in a number of steps bounded by L :

$$C_L = \{F : \text{for some index } f \text{ of } F, \Phi_f(x) \leq L(x)$$

for all sufficiently large $x\}$.

These complexity classes organize the recursive functions according to computational difficulty. In particular, we can say that F is no harder to compute than G if F belongs to every complexity class to which G belongs. This happens iff for every index of G there exists an index of F that is almost always just as fast.

5. Oracles and functionals

Three years after his original paper (TURING [1936]), TURING [1939] introduced an extension of his concept of computability. Imagine a

computing agent (an industrious clerk or a machine) provided, as usual, with explicit instructions and plenty of scratch paper. But in addition we now provide a new feature: an oracle for a particular function α from $\mathbb{N}$ into $\mathbb{N}$. (Here $\text{dom } \alpha$ is required to be all of $\mathbb{N}$; let $\mathbb{N}^{\mathbb{N}}$ be the set of all such functions.) An oracle for α is a device that, given a number x , responds by producing the value $\alpha(x)$. For a recursive α , we can make an oracle for α from a Turing machine. But more generally we can imagine an oracle for an arbitrary function α . Our computing agent supplied with this oracle now can calculate not only the effectively computable partial functions, but can further calculate (when given the right instructions) any partial function that is “computable in α ”.

At first glance, the concept of computability in α seems quite odd. It combines the most constructive approach to functions (that of computability) with the least constructive approach (that of an oracle). But despite this paradoxical appearance, the concept has proved to be valuable. And it led eventually (in the 1950's) to the concept of a recursive functional, i.e., a recursive function accepting members of $\mathbb{N}^{\mathbb{N}}$ as arguments.

In general we will consider (k, m) -place partial functions; the domain of such a function is a subset of

$$\mathcal{N} = \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N} \times \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \times \cdots \times \mathbb{N}^{\mathbb{N}}$$

(with k factors of $\mathbb{N}$ and m factors of $\mathbb{N}^{\mathbb{N}}$) and its range is a subset of $\mathbb{N}$. Until now, we have discussed only the case where the space $\mathcal{N}$ was countable (i.e., $m = 0$). Henceforth we will often treat the case $k = m = 1$ for notational simplicity, with the understanding that the remarks generalize. We use $x, y, \dots$ as variables over the space $\mathcal{N}$.

We now extend our notion of Turing machines to allow for m oracles. A machine can now write a number x on the tape and the oracle will, in one step, replace it with $\alpha(x)$. A partial function f on $\mathcal{N}$ is defined to be *recursive* if there is a Turing machine that computes f as before, where now the function arguments of f are supplied in the form of oracles.

As in Section 4, it is possible to encode the entire history of a single calculation into one number y , the computation record. Among other things, y encodes all information supplied by the oracle. Of course in any one terminating calculation, only a finite amount of the potentially infinite wisdom of the oracles can be utilized. Under any reasonable encoding of calculations, if y is a computation record then any value $\alpha(i)$ supplied to the calculation by the oracle will have $i < y$. Define for α in $\mathbb{N}^{\mathbb{N}}$ the “course-of-values” function $\bar{\alpha}$ by

$$\bar{\alpha}(y) = \langle \alpha(0), \alpha(1), \dots, \alpha(y-1) \rangle.$$

Thus $\bar{\alpha}$ is again in $\mathbb{N}^{\mathbb{N}}$ and $\bar{\alpha}(y)$ encodes the first y values of α . (In particular $\bar{\alpha}(0) = \langle \rangle = 1$, no matter what α is.) For a computation record y , the number $\bar{\alpha}(y)$ encodes all values of α that were used in the calculation, since for $i < y$ the value $\alpha(i)$ can be decoded from $\bar{\alpha}(y)$, in fact $\alpha(i) = (\bar{\alpha}(y))_i$. This phenomenon leads to the following two results.

(i) There is a recursive 4-ary relation T that holds of the natural numbers $e, \langle x_1, \dots, x_k \rangle, \langle \bar{\alpha}_1(y), \dots, \bar{\alpha}_m(y) \rangle$, and y iff e encodes a Turing machine and y is a computation record for that machine, started with $\langle x_1 \rangle 0 \langle x_2 \rangle 0 \dots 0 \langle x_k \rangle$ on the tape and supplied with oracles for $\alpha_1, \dots, \alpha_m$.

(ii) There is a recursive function U such that whenever T holds of the above-mentioned four numbers, then $U(y)$ is the output value of the calculation.

Thus we can extend the normal form results of the preceding section by defining the (k, m) -place partial function $\{e\}^{k,m}$ where

$$\{e\}^{1,1}(x, \alpha) = U(\mu y T(e, \langle x \rangle, \langle \bar{\alpha}(y) \rangle, y)).$$

As usual, we omit the superscripts whenever possible. The Normal Form Theorem 4.1 then holds, *mutatis mutandis*. It is interesting to note that since U and T have only natural numbers as arguments, recursiveness on $\mathcal{N}$ can be characterized in terms of recursiveness on $\mathbb{N}$.

6. Recursive enumerability

We have defined a subset of $\mathcal{N}$ to be a recursive (k, m) -ary relation if its characteristic function was recursive. By Church's thesis, this is the correct formalization of the informal notion of a decidable set.

Now we want to consider sets that are only half recursive. Call a set R *semi-decidable* if there is an effective procedure that, given x , replies "yes" iff $x \in R$. The procedure is no longer required to be a decision procedure; now it can be thought of as an accepting procedure. If $x \in R$, then the procedure eventually says "yes", thereby accepting x . But if $x \notin R$, then in general the procedure will never terminate. But one never knows in advance whether the procedure will go on forever or will eventually halt and accept x .

When $\mathcal{N}$ is a countable space, we can give another characterization of the semi-decidable sets. Call R *effectively enumerable* if there is an effective procedure that lists, in some order, the members of R . (Of course if R is infinite then the list will never be completed. But for any particular member of R , it appears on the listing after some finite length of time.) To prove that effective enumerability is equivalent to semi-decidability, first

assume that R is effectively enumerable. Then given any x , we can scan the listing of R as it appears, and say “yes” if and when we see x . This shows that R is semi-decidable. Conversely assume that R is semi-decidable. To generate a listing of R , we must budget our time sensibly. Order $\mathbb{N}^k$ first according to maximum component and then lexicographically; this orders $\mathbb{N}^k$ in type ω . Then go through all k -tuples in order: $x_1, x_2, \dots$. At stage n of the listing procedure, spend n minutes on each of $x_1, x_2, \dots, x_n$, testing them for acceptance into R . If any of these tests results in a “yes”, then put that k -tuple on the output list. In this way, any member of R is eventually discovered and placed on the list. (Obviously this argument relies on having a countable space $\mathbb{N}^k$; an uncountable semi-decidable set cannot be listed in this sense.)

Next we want to give a precise counterpart of the informal concept of a semi-decidable set. One possibility would be to go back to Turing machines, regarding them not as transducers (with both input and output) but as acceptors. But there is a simpler alternative open to us. Any semi-decidable set is the domain of the computable partial function taking the value 0 on the set and undefined outside the set. Conversely, the domain of any computable partial function is semi-decidable; one says “yes” if and when the computation terminates. Hence we can formulate semi-decidability as follows.

6.1. DEFINITION. A subset of $\mathcal{N}$ is *semi-recursive* if it is the domain of some recursive partial function on $\mathcal{N}$. If $\mathcal{N}$ is countable, then semi-recursive sets are called *recursively enumerable* (abbreviated r.e.).

If R is semi-recursive by virtue of being the domain of f , then we can think of the Turing machine that computes f as being the accepting device for R , where acceptance amounts to halting. The phrase “recursively enumerable” is sometimes used as a synonym for “semi-recursive” regardless of the size of $\mathcal{N}$, but we will confine the phrase to countable $\mathcal{N}$.

If we have an accepting device for R and another for its complement (with respect to $\mathcal{N}$), then the two devices together decide membership in R . Hence we have the following result.

6.2. THEOREM. A relation is recursive iff both it and its complement are semi-recursive.

We can exploit our indexing of recursive partial functions to obtain an indexing of the semi-recursive sets. Simply define W_e^k to be the domain of

$\{e\}^{k,m}$. (We omit the superscripts whenever possible.) Then a relation R is semi-recursive iff it is W_e for some e . Furthermore the $(k+1, m)$ -ary relation

$$Q = \{(e, \mathbf{x}): \mathbf{x} \in W_e\}$$

is semi-recursive (being the domain of the function computed by a universal Turing machine). The semi-recursive relation Q is "universal" for (k, m) -ary semi-recursive relations in the sense that a relation R is semi-recursive iff it is obtainable from Q by holding e fixed as a parameter.

6.3. THEOREM. *The following conditions on a (k, m) -ary relation are equivalent.*

(i) R is semi-recursive.

(ii) For some recursive $(k+1, m)$ -ary relation Q ,

$$R = \{\mathbf{x}: \exists w Q(w, \mathbf{x})\}.$$

(iii) For some recursive $(k+1, m)$ -ary relation P ,

$$R = \{\mathbf{x}: \exists w_1 \cdots \exists w_l P(w_1, \dots, w_l, \mathbf{x})\}.$$

PROOF. We have (i) $\Rightarrow$ (ii) because $x \in W_e \Leftrightarrow \exists y T(e, \langle x \rangle, y)$. Trivially (ii) $\Rightarrow$ (iii). To prove (iii) $\Rightarrow$ (i) we use sequence encoding: $R = \text{dom } f$ where $f(\mathbf{x}) = \mu w P((w)_1, (w)_2, \dots, (w)_l, \mathbf{x})$. For recursive P , the partial function f is also recursive. $\square$

In Section 4 we showed that the set

$$K = \{x: \{x\}(x) < \infty\}$$

was not recursive. But K is a recursively enumerable subset of $\mathbb{N}$, since

$$x \in K \Leftrightarrow \exists y T(x, \langle x \rangle, y)$$

for a recursive relation T . So we may conclude that the complement $\bar{K}$ is not r.e.

Although K is undecidable, there is a sense in which questions about membership in any r.e. subset of $\mathbb{N}$ are reducible to questions about K . Consider any r.e. subset W_e of $\mathbb{N}$ and define for each x the function

$$f(t) = \{e\}(x).$$

Then $f(t)$ is independent of t , and in fact f is the empty function if $x \notin W_e$. But f is total if $x \in W_e$. Now f is a recursive partial function, but more to the point is that we can recursively find an index $\pi(e, x)$ for f . On an

informal level, this is clear: the equation displayed above tells how to calculate f , and we can arrive at this equation effectively when given e and x . Formally, we use the parameter theorem below.

If g is a two-place recursive partial function, then $g(8, y)$ is, as a function of y , recursive. A more significant fact is that we can recursively find an index for this function from an index for g . This fact, stated more generally, is the following theorem.

6.4. PARAMETER THEOREM. *For each k and m there is a one-to-one total recursive function ρ such that*

$$\begin{aligned} \{e\}(x_1, \dots, x_n, y_1, \dots, y_k, \alpha_1, \dots, \alpha_m) &= \\ &= \{\rho(e, \langle x_1, \dots, x_n \rangle)\}(y_1, \dots, y_k, \alpha_1, \dots, \alpha_m) \end{aligned}$$

always holds.

Here $x_1, \dots, x_n$ are parameters being held fixed. The idea is to have $\rho(e, v)$ encode instructions for writing v to the left of the other input on the tape, and then following instruction encoded by e . (The parameter theorem is also known as the “S–m–n theorem”, for historical reasons.)

We can now apply the parameter theorem to the function

$$g(e, x, t) = \{e\}(x)$$

to get a one-to-one total recursive π such that $g(e, x, t) = \{\pi(e, x)\}(t)$ and hence

$$x \in W_e \Rightarrow \{\pi(e, x)\} \text{ is total,}$$

$$x \notin W_e \Rightarrow \{\pi(e, x)\} \text{ is empty,}$$

$$x \in W_e \Leftrightarrow \pi(e, x) \in K.$$

This reduces questions about W_e to questions about K . There are other r.e. sets besides K for which such reductions exist. The most obvious example is $\{\langle x, y \rangle : x \in W_y\}$.

For subsets A and B of $\mathbb{N}$, define A to be *many-one reducible* to B ($A \leq_m B$) if for some total recursive f ,

$$x \in A \Leftrightarrow f(x) \in B.$$

Call A *one-one reducible* to B ($A \leq_1 B$) if in addition f can be required to be one-to-one. Then any r.e. subset of $\mathbb{N}$ is one-one reducible to K . It is clear (at least on the informal level) that if either $A \leq_m B$ or $A \leq_1 B$ and B is recursive, then A is also recursive. The same is true with “recursive” replaced by “recursively enumerable”.

The parameter theorem is a standard tool in formalizing reductions of one decision problem to another. Such a reduction may prove that a decision problem is unsolvable, as in the following result.

6.5. THEOREM (RICE [1953]). *Let $\mathcal{C}$ be a set of one-place recursive partial functions. Then the set $\{e: \{e\} \in \mathcal{C}\}$ of indices of members of $\mathcal{C}$ is recursive iff either $\mathcal{C}$ is empty or $\mathcal{C}$ contains all one-place recursive partial functions.*

PROOF. The " $\Leftarrow$ " half is trivial. So assume that the set of indices

$$I = \{e: \{e\} \in \mathcal{C}\}$$

is recursive. Since both the hypothesis and the conclusion of the theorem are symmetric with respect to $\mathcal{C}$ and its complement, we may suppose that the empty function $\emptyset$ is not in $\mathcal{C}$. We will show that $\mathcal{C}$ is empty by showing that we could otherwise reduce membership questions about K to the recursive set I .

So assume that, contrary to our hopes, some function ψ is in $\mathcal{C}$. The idea is to end up with $x \in K \Leftrightarrow g(x) \in I$ by arranging to have $\{g(x)\}$ be ψ or $\emptyset$ as x either is or is not in K . Informally, $g(x)$ encodes instructions for: given y , compute first $\{x\}(x)$ and then $\psi(y)$. Formally, $g(x) = \rho(e, \langle x \rangle)$ where

$$\{e\}(x, y) = U(\mu z [T(x, \langle x \rangle, (z)_0) \ \& \ T(q, \langle y \rangle, (z)_1)]),$$

and q is an index for ψ . This gives us $K \leq_1 I$, contradicting the fact that I is recursive and K is not. $\square$

As immediate consequences of Rice's theorem, we have the following negative statements. The set of indices of total recursive functions is not recursive. For any fixed recursive partial function f on $\mathbb{N}$, the set of indices of f is not recursive (and hence is infinite). The set $\{e: W_e \text{ is finite}\}$ is not recursive. And so forth.

A more subtle consequence of the parameter theorem is the recursion theorem, due to KLEENE [1938].

6.6. RECURSION THEOREM. (i) *For any total recursive $f: \mathbb{N} \rightarrow \mathbb{N}$ we can find a number e for which $\{e\} = \{f(e)\}$.*

(ii) *For any recursive partial function g we can find a number e such that $\{e\}(\bar{x}) = g(e, \bar{x})$ for all $\bar{x}$.*

The proof is very like the proof that gives us self-referential sentences in number theory (e.g. Theorem 2.2.1 in Chapter D.1).

PROOF. Parts (i) and (ii) are equivalent. To prove (i), we obtain from the parameter theorem a total recursive γ such that $\{\gamma(x, y)\} = \{\{x\}(y)\}$ for any x and y . Let r be an index for the function whose value at x is $f(\gamma(x, x))$ and let $e = \gamma(r, r)$. This number e works:

$$\{e\} = \{\gamma(r, r)\} = \{\{r\}(r)\} = \{f(\gamma(r, r))\} = \{f(e)\}.$$

To prove part (ii), we first get from the parameter theorem a total recursive f such that $\{f(t)\}(\mathfrak{x}) = g(t, \mathfrak{x})$. Then by part (i) there is a number e such that $\{e\}(\mathfrak{x}) = \{f(e)\}(\mathfrak{x}) = g(e, \mathfrak{x})$. $\square$

We can use the recursion theorem to give a short proof of Rice's theorem. Suppose that $\{a\} \in \mathcal{C}$ and $\{b\} \notin \mathcal{C}$, and define $f(x)$ to be b or a as x is or is not in I . There can be no e such that $\{e\} = \{f(e)\}$, and hence f cannot be recursive. So I is not recursive.

7. Logic and recursion theory

Why is recursive function theory part of mathematical logic? If logicians had not invented recursive functions, computer scientists would have developed the subject later. But it was not a mere historical accident that recursive functions were invented by logicians. There are certain aspects of logic that inevitably involve the notions of constructiveness and effectiveness.

A basic concept of logic is that of a *proof*. Now a proof, viewed abstractly, is a series of statements that "establishes" without doubt the truth of its conclusion, given the truth of its assumptions. But to establish convincingly the truth of the conclusion, the proof must be verifiable by others. There must be some procedure by which an outsider can verify the correctness of the proof, without having to supply brilliant insight. That is, it must be possible to verify the correctness of proofs by an effective procedure. The set of proofs must be recursive. It would not do, for example, to consider just any series of true sentences of arithmetic to be a proof of its last line. We cannot, given a sentence of arithmetic, tell effectively whether or not it is true, because the set of true sentences of arithmetic is not recursive nor even r.e. (Section 10).

Now consider the set of all theorems, i.e., the provable sentences. A sentence σ is provable iff

$$\exists d [d \text{ is a proof of } \sigma].$$

The part in square brackets must be recursive. And so the set of theorems must be recursively enumerable. Thus as long as we can effectively recognize correct proofs, the set of theorems will be recursively enumerable! The Gödel incompleteness theorem discussed in Chapter D.1 stems from the fact that provability is r.e. whereas truth is not.

To be more specific, consider a first-order language L , such as the language for set theory, having finitely many non-logical symbols. (Actually there could be $\aleph_0$ non-logical symbols as long as they are arranged tidily.) We first assign numbers (called *Gödel numbers*) to the expressions of the language in a straightforward way. This permits us to apply notions of recursion theory to the expressions. (Alternatively we could have Turing machines work directly on the symbols of the language.) In fact we will not bother to distinguish between an expression and its Gödel number. One can verify that the set of formulas is recursive, as is the set of sentences. Now add a set A of axioms, such as the Zermelo–Fraenkel (ZF) axioms of set theory. We naturally expect A to be recursive, so that in verifying the correctness of a proof we will be able effectively to tell the axioms from the non-axioms. (For example, the set of ZF axioms is recursive.) For a recursive set A , the binary relation

$$\{(\sigma, d): d \text{ is a proof of } \sigma \text{ from } A\}$$

is recursive, where “proof” is defined as in Section 4 of Chapter A.1. (In fact we could use either formal system from that chapter.) This is not a deep result; we intuitively expect proofhood to be decidable, so when the concepts involved are made precise it should not be surprising to find that it is indeed decidable. Call a theory *recursively axiomatizable* if it is given by a recursive set A of axioms in a language L as above.

7.1. THEOREM. *A recursively axiomatizable theory has a recursively enumerable set of theorems*

PROOF. τ is a theorem iff

$$\exists d [d \text{ is a proof of } \tau \text{ from } A]$$

where A is the recursive set of axioms. The part in brackets is recursive. $\square$

Take again the example of ZF set theory. By Theorem 7.1, the set of theorems of ZF is r.e. It follows that the sentences of arithmetic provable in ZF (this can be made precise) form a r.e. set. So they cannot coincide with

the true sentences of arithmetic. Either too much is provable (and ZF is lying to us) or too little is provable.

Now let us go one step further and suppose that we have a recursively axiomatizable theory that is complete (i.e., for any sentence σ , either σ or $(\neg\sigma)$ is a theorem). Then we can strengthen Theorem 7.1; the theory is actually decidable.

7.2. THEOREM. *A complete recursively axiomatizable theory has a recursive set of theorems.*

PROOF. The conclusion certainly holds if the theory is inconsistent, so assume the theory is consistent. Suppose we are given a sentence σ and we want to decide whether it is a theorem. We generate a listing of all the theorems; by Theorem 7.1 this is possible. Eventually either σ or $(\neg\sigma)$ appears in the listing. When this happens, we can stop and give the correct answer. $\square$

Theorem 7.2 is the basis for a number of decidability results; see Chapter C.3. Of course it suffers from the limitation of being applicable only to theories that are complete.

Properly viewed, proofs and calculations are objects of the same sort. A calculation (written down with all the steps) is a proof that the value of a function of a given argument is a certain number. And a proof is a calculation of one value of the function whose domain is the set of theorems. It is a calculation in the sense of being a finite and verifiable record that correct procedures have been followed.

For example, it turns out that a set R of numbers is recursive iff it is binumerable in first-order Peano arithmetic (cf. Section 3). Here the role of Turing machine computations is played by the formal deductions, *modus ponens* and all, establishing that a given number is indeed in the set.

Turing machines themselves have proved to be convenient tools in a variety of undecidability problems in logic. Take for example the result of KAHR, MOORE and WANG [1962] that for any formula φ we can effectively find an $\forall\exists\forall$ formula that is satisfiable iff φ is satisfiable. This is *not* proved by syntactical manipulations on φ , but instead by finding for each Turing machine M an $\forall\exists\forall$ formula that is satisfiable iff M never halts. This, together with results of the previous section, yields the existence of the desired reduction.

Or suppose we want to prove that the set of sentences having models of every non-zero cardinality is undecidable. We can do this by showing how,

given a Turing machine M , to find effectively a sentence that has models of every non-zero cardinality iff M never halts.

8. Degrees of unsolvability

All of the non-recursive sets have unsolvable decision problems. But some are more unsolvable than others. In this section we will see how some amount of order can be imposed on the unsolvable problems.

Consider a partial function f on $\mathcal{N}$, and let $\mathcal{B}$ be a subset of $\mathbb{N}^{\mathbb{N}}$. It may be possible to compute f if we are given oracles for each function in $\mathcal{B}$. Define f to be *recursive in $\mathcal{B}$* if there exists some recursive partial function g and some $\beta_1, \dots, \beta_n$ in $\mathcal{B}$ such that

$$f(\mathfrak{x}) = g(\mathfrak{x}, \beta_1, \dots, \beta_n)$$

for all $\mathfrak{x}$. Other definitions can then be “relativized to $\mathcal{B}$ ”. For example a subset of $\mathcal{N}$ is *recursive in $\mathcal{B}$* if its characteristic function is recursive in $\mathcal{B}$, and it is *semi-recursive in $\mathcal{B}$* if it is the domain of some partial function recursive in $\mathcal{B}$. Usually $\mathcal{B}$ will be a singleton $\{\beta\}$, so that we speak of recursiveness in β and so forth.

The extreme case of $\mathcal{B} = \mathbb{N}^{\mathbb{N}}$ deserves special mention. When we give ourselves oracles for all functions in $\mathbb{N}^{\mathbb{N}}$, matters of recursiveness are washed out. On a countable space $\mathcal{N}$, every function is recursive in $\mathbb{N}^{\mathbb{N}}$. But for uncountable $\mathcal{N}$ this does not happen. If f is recursive in $\mathbb{N}^{\mathbb{N}}$ then in calculating $f(\alpha)$ there is still one restriction: We can use only a finite amount of information about α . That is, there must be some y (depending on α) such that $f(\alpha) = f(\gamma)$ for any γ agreeing with α at the first y values. This is exactly the condition for f to be continuous, when we put the discrete topology on $\mathbb{N}$ and the product topology on $\mathbb{N}^{\mathbb{N}}$. The space $\mathcal{N}$ is then given the product topology.

8.1. THEOREM. (a) *A function on $\mathcal{N}$ is recursive in $\mathbb{N}^{\mathbb{N}}$ iff it is continuous.*
 (b) *A subset of $\mathcal{N}$ is semi-recursive in $\mathbb{N}^{\mathbb{N}}$ iff it is open.*

All the uncountable spaces $\mathcal{N}$ are homeomorphic to $\mathbb{N}^{\mathbb{N}}$. For example a homeomorphism from $\mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$ onto $\mathbb{N}^{\mathbb{N}}$ can map (α, β) to the function taking $2x \mapsto \alpha(x)$ and $2x+1 \mapsto \beta(x)$. And $\mathbb{N}^{\mathbb{N}}$ is homeomorphic to the irrationals; the mapping here uses continued fractions. Thus it is possible to give a uniform treatment of topological set theory of the irrationals on the one hand and recursion theory of $\mathcal{N}$ on the other. Both sides gain from this

connection For further discussion on this vein, see Chapter C.8 on descriptive set theory.

But we have strayed from our main topic. We will be concerned with a special case of relative recursiveness. Let α and β be members of $\mathbb{N}^{\mathbb{N}}$. Then, by our previous definition, α is recursive in β iff there is a recursive partial function g for which

$$\alpha(x) = g(x, \beta).$$

(Although both α and β are total, we cannot demand that g be total.) If α is recursive in β , then we write $\alpha \leq_{\tau} \beta$ and say that α is *Turing reducible* to β . We can also (and in fact equivalently) work with subsets of $\mathbb{N}$: say that A is recursive in B (written $A \leq_{\tau} B$) if the characteristic function of A is recursive in the characteristic function of B .

8.2. THEOREM. *The binary relation $\leq_{\tau}$ (either on $\mathbb{N}^{\mathbb{N}}$ or on $\mathcal{P}(\mathbb{N})$) is reflexive and transitive.*

On an informal level, transitivity of $\leq_{\tau}$ corresponds to connecting machines in series.

As a consequence of the above theorem, the symmetric relation of Turing equivalence

$$\alpha \equiv_{\tau} \beta \quad \text{iff} \quad \alpha \leq_{\tau} \beta \text{ and } \beta \leq_{\tau} \alpha$$

is an equivalence relation on $\mathbb{N}^{\mathbb{N}}$. Let $[\alpha]$ be the equivalence class of α . The equivalence classes are called *degrees of unsolvability*. The degrees are partially ordered by the relation

$$[\alpha] \leq [\beta] \quad \text{iff} \quad \alpha \leq_{\tau} \beta.$$

(Clearly this is well defined on equivalence classes.) We get the same degree structure on $\mathcal{P}(\mathbb{N})$ as on $\mathbb{N}^{\mathbb{N}}$, since for any α we can find a set B with α Turing equivalent to the characteristic function of B .

Thus the degrees of unsolvability are partially ordered according to just how unsolvable they are. There is obviously a least degree $\mathbf{0}$, consisting of the recursive functions. Because for any fixed function β the set $\{\alpha : \alpha \leq_{\tau} \beta\}$ is countable, it follows that each degree is a countable set of functions. Consequently there are $2^{\aleph_0}$ degrees. Another consequence is that any chain of degrees — any linearly ordered subset — has cardinality at most $\aleph_1$. This strongly suggests that incomparable degrees exist. This suspicion can be proved to be correct (without having to deny the

continuum hypothesis). We can simultaneously construct α and β so as to sabotage each machine that might reduce one function to the other.

In fact much more is true. There is an antichain — a set of degrees no two of which are comparable — of cardinality $2^{\aleph_0}$. This result is just a piece of the extensive information known about the degrees. See Chapter C.4 for much more on this topic.

Call a degree *recursively enumerable* (r.e.) if it is the degree of some r.e. set. Recall that the set

$$K = \{x: \{x\}(x) < \infty\}$$

is a r.e. subset of $\mathbb{N}$ that is not recursive. Hence the degree of K , denoted $\mathbf{0}'$, is a r.e. degree greater than $\mathbf{0}$. In Section 9 we will consider the question whether there are other r.e. degrees (Post's problem).

The passage from $\emptyset$ to K can be relativized to give us a function $A \mapsto A'$ on $\mathcal{P}(\mathbb{N})$. Define the *jump* of A (denoted A') to be the set

$$\{x: \{x\}^A(x) < \infty\}$$

where $\{x\}^A$ is the partial function recursive in A with index x , i.e.,

$$\{x\}^A(y) = \{x\}(y, \chi_A)$$

where χ_A is the characteristic function of A . Then A' is r.e. in A , but is not recursive in A ; the proof is the same as for K . In fact by relativizing the proof of the corresponding result for K we have the following.

8.3. THEOREM. (i) A' is r.e. in A but is not recursive in A .

(ii) A set B is r.e. in A iff $B \leq_1 A'$.

Thus among the sets that are r.e. in A , its jump A' ranks highest with respect to one-one reducibility. It follows from the foregoing theorem that the jump operation is well defined on degrees.

8.4. THEOREM. $A \leq_T B$ iff $A' \leq_1 B'$.

This lets us define for each degree $\mathbf{a}$ its jump $\mathbf{a}'$. By Theorem 8.3 we have $\mathbf{a} < \mathbf{a}'$. And so we can continue: $\mathbf{a} < \mathbf{a}' < \mathbf{a}'' < \dots$. In particular there is no largest degree. And above any degree we can find a chain of order type ω . In fact we can find one of the order type of the first uncountable ordinal; at limit ordinal steps we gather together all the previous sets in some systematic way.

9. Creative and lesser sets

As observed in Section 7, any recursively axiomatizable theory has a r.e. set of theorems. Thus r.e. sets are of particular significance for logic. For example one could hope that by classifying r.e. sets one would obtain an interesting classification of axiomatizable theories. The binary classification of r.e. sets into the recursive and non-recursive sets partitions theories into decidable and undecidable theories. But one could hope for a refinement of this binary split.

The first classification to examine comes from the degrees of unsolvability. And next one could examine the refinement obtained from other reducibilities. Clearly

$$A \leq_1 B \Rightarrow A \leq_m B \Rightarrow A \leq_T B,$$

so when we define

$$A \equiv_1 B \quad \text{iff} \quad A \leq_1 B \ \& \ B \leq_1 A,$$

$$A \equiv_m B \quad \text{iff} \quad A \leq_m B \ \& \ B \leq_m A$$

the equivalence relation $\equiv_T$ is refined by $\equiv_m$ and further refined by $\equiv_1$. Section 6 shows that there is a largest r.e. degree (the degree of K) with respect to each of these reducibilities.

But what about the other r.e. degrees? Each such degree contains axiomatizable theories:

9.1. THEOREM (FEFERMAN [1957]). *Every r.e. degree of unsolvability contains a recursively axiomatizable theory.*

PROOF. For any set A of numbers we can form a theory in the language of equality by taking as axioms the set

$$\{\neg \varepsilon_n : n \in A\}$$

where ε_n is the sentence “there are exactly n things in the universe”. Then the set of theorems is Turing equivalent to A . If A is r.e. then we certainly have a r.e. set of axioms. But any theory whose axioms can be recursively enumerated $\{\sigma_0, \sigma_1, \sigma_2, \dots\}$ has a recursive set of axioms $\{\sigma_0, \sigma_0 \wedge \sigma_1, \sigma_1 \wedge \sigma_1 \wedge \sigma_2, \dots\}$. $\square$

HANF [1965] has shown that this theorem can be strengthened by requiring that the theory be finitely axiomatizable. But the effect of the theorem is offset by the empirical observation that all “natural” r.e.

theories are either of degree 0 or of degree $0'$. Proofs that a theory T is undecidable generally show, in effect, that the halting problem for Turing machines is reducible to T . And the reducibility here is (or can become) $\leq_1$, so that the proof shows that $K \leq_1 T$. If T is recursively axiomatizable, then we have $T \equiv_1 K$.

For the cases of $\equiv_1$ and $\equiv_m$ we can give an intrinsic characterization of the sets in the highest r.e. degree. Theorem 6.2 states that a r.e. set A is non-recursive iff each r.e. subset of its complement $\bar{A}$ fails to fill $\bar{A}$. By uniformizing this last condition, we obtain the following definition, due to Post [1944].

9.2. DEFINITION. A set A of numbers is *creative* if A is r.e. and there exists a recursive partial function f such that whenever $W_x \subseteq \bar{A}$ then $f(x) \in \bar{A} - W_x$.

The function f in this definition is called a *productive* function for $\bar{A}$. For example, our set K is creative; we can take $f(x) = x$.

9.3. THEOREM (MYHILL [1955]). *The following conditions on a set of numbers are equivalent.*

- (i) A is creative.
- (ii) A is a r.e. set to which all r.e. sets are $\leq_1$ -reducible.
- (iii) A is a r.e. set to which all r.e. sets are $\leq_m$ -reducible.

Trivially (ii) $\Rightarrow$ (iii) and it is not hard to show that (iii) $\Rightarrow$ (i). The main part of the proof is establishing (i) $\Rightarrow$ (ii). This breaks down into two steps, first showing that a creative set has a one-to-one total productive function, and secondly using a version of the recursion theorem.

The above theorem implies that the usual undecidable axiomatizable theories such as first-order Peano arithmetic have creative sets of theorems.

There is still the question of what (if anything) lies between the recursive sets and the creative sets. For $\leq_m$ and $\leq_1$ reducibilities, the existence of intermediate sets was established by Post [1944]. He noted that a creative set must have a very rich complement, and proceeded to construct sets with sparse complements. Call a r.e. set S *simple* if $\bar{S}$ is infinite but includes no infinite r.e. subset.

9.4. THEOREM (POST [1944]). *Simple sets exist.*

PROOF. Imagine a fixed method of enumerating all r.e. sets. For each n , put into S the first discovered (if any) member of W_n that is greater than $2n$.

Then S is r.e., S intersects every infinite r.e. set, but S contains at most n of the first $2n + 1$ numbers. $\square$

A simple set is obviously non-recursive. And it is easy to generate an infinite r.e. subset of the complement of any creative set, so a simple set cannot be creative. Thus the above theorem establishes the existence of r.e. sets of intermediate $\equiv_m$ and $\equiv_1$ degree. "Post's problem" is the question whether there are r.e. sets of Turing degree intermediate between 0 and $0'$. This question is not answered by the simple sets, which can be of degree $0'$. Post had hoped that by placing even more stringent requirements on $\bar{S}$, he could force S to be of intermediate degree of unsolvability. This approach turned out to be unsuccessful. Finally in 1956 (two years after Post's death) the problem was solved simultaneously and independently by Friedberg (in his senior thesis at Harvard and in FRIEDBERG [1957]) and MUČNIK [1956] in the Soviet Union. They showed that intermediate r.e. degrees do exist, and in great profusion. Their method of proof has been termed the "priority method". In broad terms, this method involves a construction in which there are infinitely many requirements to be satisfied. But some of these requirements conflict with one another, so at various stages of the construction one must satisfy requirements of high priority, allowing those of lower priority to be injured. If all goes well, at the end each requirement has received enough attention for the construction to succeed.

Since 1956 the r.e. degrees have been studied extensively. We will quote here two theorems, both due to SACKS [1964, 1963]. The r.e. degrees are dense, in that if $\mathbf{a} < \mathbf{c}$ then $\mathbf{a} < \mathbf{b} < \mathbf{c}$ for a third r.e. degree $\mathbf{b}$. And any countable partial ordering can be embedded in the partial ordering of r.e. degrees. (For this it suffices to embed some countable atomless Boolean algebra — as a partial ordering — in the r.e. degrees.)

10. Definability and recursion

Mathematics is, as it has always been, largely the science of measurement. But "measurement" must here be understood as referring to more than the meter stick. The genus of a topological figure measures one of its aspects; objects of genus zero are in a sense simpler than those of higher genus. There are many dimensions of measurement in mathematics, and they go by many names: characteristic, transcendence degree, cardinality, fundamental group, etc. Occasionally we are so successful in the science of measurement that we can completely characterize an object (at least to

within some concept of isomorphism) by giving, as it were, its latitude and longitude, i.e., its measurements in the relevant dimensions.

Usually the measurement values in a particular dimension can be ordered or at least partially ordered. They then induce a ranking on the objects being measured, according to whether the measurement of the object yields a value that is small or large.

Now consider the case of measurement of sets of natural numbers. This case is not as specialized as it might seem, since it is applicable to anything that can be encoded into sets of numbers, such as formal languages (sets of strings of symbols). First of all we have a binary measurement: a set of numbers can be recursive or non-recursive. For example the set of primes is recursive, and the set of theorems of set theory or group theory, suitably encoded, is not recursive. There are countably many recursive sets, so almost all sets (in the usual measure on $\mathcal{P}(\mathbb{N})$) are non-recursive.

The degrees of unsolvability provide one scale of measurement, indicating how far a set is from being recursive. But the degrees themselves form an untidy array, with only a few reliable bench marks to help us get our bearings.

The scale of measurement to be treated in this section is definability. It is applicable, in the present context, to sets that are definable in the structure $\mathfrak{N} = (\mathbb{N}, 0, S, +, \cdot)$ by formulas of first or second order. For each natural number n , let $\mathbf{n}$ be the corresponding numeral in the formal language of $\mathfrak{N}$. A formula $\varphi(x)$ with just x free is said to define A in $\mathfrak{N}$ if for every n ,

$$n \in A \Leftrightarrow \mathfrak{N} \models \varphi(\mathbf{n}).$$

(This notation is from Chapter A.1.) Thus A consists of exactly those numbers making φ true in $\mathfrak{N}$. In the case of a k -ary relation, we use a formula $\varphi(x_1, \dots, x_k)$ with several free variables.

Obviously only countably many sets are definable. We can produce an artificial example of a non-definable set by diagonalization. Nevertheless, among the $\aleph_0$ sets that are definable in $\mathfrak{N}$ lie most of the interesting sets of numbers. After all, if we are interested in A , then we probably know what A is, and that knowledge can probably be formalized to yield a definition of A in $\mathfrak{N}$.

If a set is definable in $\mathfrak{N}$, then we want to have a measurement indicating *how* definable it is. For a start, call a set *arithmetical* if it is definable in $\mathfrak{N}$ by a first-order formula, and call it *analytical* if it is definable by a second-order formula. Then the arithmetical sets constitute a subclass of the analytical sets, and it is a subclass of sets that are more easily definable than are the sets in its complement.

Within the class of arithmetical (or analytical) sets, we can ask for finer measurements as to just how definable a given set is. For example, we could use as a measurement the length of the shortest defining formula, or the number of quantifiers. But to obtain intrinsically significant measurements, some care is needed.

For example, exponentiation (as a ternary relation) is definable in $\mathfrak{N}$. But it is not easy to find a defining formula, and any defining formula will be fairly long. Yet our decision to include addition and multiplication in $\mathfrak{N}$ and to exclude exponentiation was rather arbitrary. We want measurements that are free from such arbitrary choices. For this reason we decide to measure “definability modulo recursiveness”. We have available the following theorem, which is essentially due to GÖDEL [1931].

10.1. THEOREM. *Every recursive relation on $\mathbb{N}$ is arithmetical.*

The proof uses the techniques of Section 4 to translate statements about Turing machines into statements about numbers. It is necessary to have an arithmetical way of encoding a sequence of numbers into a single number. The Chinese remainder theorem provides such a method.

From this theorem we can further conclude that r.e. relations on $\mathbb{N}$ are also arithmetical, since the defining formula for $\{x: \exists y R(x, y)\}$ requires only one quantifier more than the defining formula for R . And complements of r.e. relations are arithmetical, and so forth.

Before making that “and so forth” more systematic, we should note that we can now prove the undecidability of number theory. Let T be the set of sentences true in $\mathfrak{N}$, suitably encoded into numbers. The set K is arithmetical, and so for some formula φ , we have $x \in K$ iff $\varphi(x) \in T$. But this yields $K \leq_1 T$, so T cannot be recursive. We will see presently that a modification of this argument shows that T is not even arithmetical.

To return to definability, note that another consequence of Theorem 10.1 is that the arithmetical relations on $\mathbb{N}$ are exactly those definable in the structure with universe $\mathbb{N}$ and with *all* recursive relations. This is the natural structure in which to measure definability modulo recursiveness. Any relation definable in this structure is of course definable by a formula in prenex form. We will use the number of alternations between universal and existential quantifiers in that prenex formula as a measure of definability.

We can formulate these ideas in the following way, and for an arbitrary space $\mathcal{N}$. Let Π_0 be the class of recursive relations. Define Σ_{n+1} to be the class of all projections of Π_n relations, where in the present context P is called a projection of R if

$$P = \{x: \exists y_1 \cdots \exists y_l R(y_1, \dots, y_l, x)\}.$$

Thus if R is a $(k + l, m)$ -ary relation, then P is a (k, m) -ary relation. We allow projection here only along numerical axes, not function axes. To complete the definition, let Π_n be the class of complements of relations in Σ_n .

An equivalent definition of Σ_n and Π_n can, at least for countable $\mathcal{N}$, be formulated in terms of the structure $\mathfrak{N}$ with universe $\mathbb{N}$ and with all recursive relations. A relation is in Σ_{n+1} iff it is definable in $\mathfrak{N}$ by a prenex formula having n alternations between universal and existential quantifiers, and whose outermost quantifier is existential. Π_{n+1} can be given a similar characterization, wherein the outermost quantifier is universal. (For uncountable $\mathcal{N}$, analogous characterizations are possible, if provision for function variables is made. We must allow formulas expressing $\bar{\alpha}(x) = y$.)

Although we have deliberately shifted from the structure $\mathfrak{N}$ to $\mathfrak{N}$, it was proved in 1970 that the above paragraph remains correct with $\mathfrak{N}$ in place of $\mathfrak{N}$. Matijacevič's theorem that solved (or rather unsolved) Hilbert's tenth problem shows that any r.e. set of numbers can be put into the form

$$\{y: \exists x (p(x, y) = q(x, y))\}$$

where $x \in \mathbb{N}^k$ and p and q are polynomials over $\mathbb{N}$. For details on this theorem, see Chapter C.2.

To return to the arithmetical hierarchy, it is convenient to define also the class

$$\Delta_n = \Sigma_n \cap \Pi_n$$

when $n \geq 1$. For example, Theorem 6.2 implies that Δ_1 is the class of recursive relations, since Σ_1 is the class of semi-recursive relations and Π_1 is the class of complements of semi-recursive relations. By using vacuous quantifiers in defining formulas we can easily establish the following inclusions.

$$\begin{array}{ccccccc} & \subset & \Sigma_1 & \subset & \subset & \Sigma_2 & \subset & \subset & \dots \\ \Delta_1 & & & & \Delta_2 & & \Delta_3 & & \\ & \subset & & \subset & \subset & \subset & \subset & & \end{array}$$

The class of arithmetical relations is the union of all these classes. All the inclusions shown above are proper. This follows from the hierarchy theorem below, due to KLEENE [1943].

10.2. THEOREM. *For each k, m , and n :*

(i) *There is a $(k+1, m)$ -ary relation in Σ_{n+1} that is universal for (k, m) -ary relations in Σ_{n+1} (i.e., every (k, m) -ary relation is obtainable by holding the first numerical variable fixed as a parameter).*

(ii) *There is a (k, m) -ary relation in Σ_{n+1} that is not in Π_{n+1} .*

Part (ii) follows from part (i) by diagonalization, and part (i) follows from the Normal Form Theorem.

It is easy to see that both Σ_n and Π_n are closed under many-one reducibility. They are not closed under Turing reducibility, since every set of numbers is recursive in its complement.

We can now extend our proof that the set T of sentences true in $\mathfrak{N}$ is not recursive, to show that T is not arithmetical. In place of K , take any Σ_{n+1} subset A of $\mathbb{N}$ that is not Π_{n+1} . Then as before $A \leq_1 T$, so T cannot be Π_{n+1} . Since n is arbitrary, T cannot be arithmetical.

We can relate the arithmetical hierarchy to the jump operation on degrees of unsolvability, thus linking the definability concepts with the ideas of Section 8. The jump operation was there characterized by an existential quantifier, which corresponds to projection of relations. This line of thought leads eventually to the theorem below, which is proved by iteration of Theorem 8.3(ii). Let $\emptyset^{(n)}$ be the result of applying the jump operation n times to $\emptyset$.

10.4. THEOREM (POST [1948]). *A subset of $\mathbb{N}$ is in Σ_{n+1} iff it is r.e. in $\emptyset^{(n)}$ (and this holds iff it is one-one reducible to $\emptyset^{(n+1)}$). It is in Δ_{n+1} iff it is recursive in $\emptyset^{(n)}$.*

Recall that the analytical sets are those definable in $\mathfrak{N}$ by formulas of second order. As in the arithmetical hierarchy, we can use the number of alternations between universal and existential quantifiers (now quantifying function variables) as a measurement of definability. Let

$$\Sigma_0^1 = \Pi_0^1 = \text{the class of arithmetical relations.}$$

Define Σ_{n+1}^1 to be the class of all projections along function axes of relations in Π_n^1 . Thus a relation in Σ_{n+1}^1 is of the form

$$\{x: \exists \alpha_1 \cdots \exists \alpha_l R(x, \alpha_1, \dots, \alpha_l)\}$$

where R is in Π_n^1 . Define Π_n^1 to be the class of complements of relations in Σ_n^1 , and define Δ_n^1 to be $\Sigma_n^1 \cap \Pi_n^1$.

The simplest facts about the arithmetical hierarchy can be extended to the analytical hierarchy. We have the inclusions:

$$\begin{array}{ccccccc} & & \subset & \Sigma_1^1 & \subset & \Sigma_2^1 & \subset & \Sigma_3^1 & \subset & \dots \\ \Delta_1^1 & & & & \Delta_2^1 & & \Delta_3^1 & & & \\ & \subset & & & \subset & & \subset & & & \\ & & \Pi_1^1 & \subset & \Pi_2^1 & \subset & \Pi_3^1 & \subset & \dots \end{array}$$

All inclusions here are proper, by a hierarchy theorem directly analogous to Theorem 10.2.

These classes in the analytical hierarchy enjoy stronger closure properties than do their counterparts in the arithmetical hierarchy. This is illustrated by Theorem 10.5 below, which is a quantitative version of the transitivity of definability. The classes Σ_n^β and $\Sigma_n^{1,\beta}$ are defined by replacing recursiveness by the relativized notion of recursiveness in β .

10.5. TRANSITIVITY THEOREM. Assume that $\mathcal{A} \subseteq \mathcal{N}$ and $\beta \in \mathbb{N}^{\mathbb{N}}$.

- (i) $\mathcal{A} \in \Sigma_{m+1}^\beta \text{ \& } \beta \in \Delta_{n+1} \Rightarrow \mathcal{A} \in \Sigma_{m+n+1}$
 (ii) $\mathcal{A} \in \Sigma_m^{1,\beta} \text{ \& } \beta \in \Delta_n^1 \Rightarrow \mathcal{A} \in \Sigma_{\max(m,n)}^1$

The proof of (i) is straightforward. The proof of (ii), due to SHOENFIELD [1962], begins by writing

$$x \in \mathcal{A} \Leftrightarrow \exists \gamma [\gamma = \beta \text{ \& } Q(x, \gamma)]$$

where Q is in Σ_m^1 . The expression on the right is then put into prenex form. Part (ii) prevents having an analogue of Post's theorem (Theorem 10.4) hold for the analytical hierarchy.

What is in Δ_1^1 ? A clue is provided by descriptive set theory. When we relativize recursiveness to $\mathbb{N}^{\mathbb{N}}$, then Σ_1^1 becomes the class of projections of Borel sets of finite rank. These are the *analytic* or *A*-sets of descriptive set theory. Souslin's theorem SOUSLIN [1917] shows that a set and its complement are both analytic iff the set is a Borel set. This suggests, by analogy, that Δ_1^1 consists of the sets obtained by extending the arithmetical hierarchy into the transfinite. This is exactly correct; the hierarchy is called the *hyperarithmetical* hierarchy. It can be constructed by suitably iterating the jump operation over all ordinals that are "recursively countable" in the sense of being the order type of some recursive well ordering of numbers.

Determining the location of a given set in these hierarchies reduces to two problems. First there is the (usually easy) matter of establishing the

positive fact that the set in question does belong to, say, Σ_2^1 . Then there is the negative task of showing that this is the best possible result, by showing that the set does *not* belong to the dual class Π_2^1 . Take for example the subset R of $\mathbb{N}^{\mathbb{N}}$ consisting of the total recursive functions from $\mathbb{N}$ into $\mathbb{N}$. Then $R \in \Sigma_3$, because

$$\alpha \in R \Leftrightarrow \exists e \forall x \exists y [T(e, \langle x \rangle, y) \ \& \ U(y) = \alpha(x)]$$

and the part in brackets is recursive. SHOENFIELD [1958] has shown that R is not in Π_3 .

We have seen that the set of true sentences of arithmetic is not arithmetical. This set does lie in the hyperarithmetical hierarchy, at level ω . This is a sharpening of Gödel's incompleteness theorem, which asserts that the set is not r.e. But now consider the characteristic function τ of the set of true sentences. Then the singleton $\{\tau\}$, as a subset of $\mathbb{N}^{\mathbb{N}}$, is in Π_2 . To prove this we look closely at the definition of satisfaction in $\mathfrak{R}$ (Definition 3.8 of Chapter A.1). Viewed as conditions on τ , the definition is a Π_2 statement that is true of τ and nothing else. Since $\{\tau\}$ is in Π_2 , it follows easily that truth is in Δ_1^1 :

$$s \text{ is true} \Leftrightarrow \forall \alpha [\alpha \in \{\tau\} \Rightarrow \alpha(s) = 1]$$

$$\Leftrightarrow \exists \alpha [\alpha \in \{\tau\} \ \& \ \alpha(s) = 1].$$

The class of well orderings of $\mathbb{N}$ can be identified with a subset of $\mathbb{N}^{\mathbb{N}}$, namely

$$\{\alpha \in \mathbb{N}^{\mathbb{N}} : \{(x, y) : \alpha(\langle x, y \rangle) = 0\} \text{ well orders } \mathbb{N}\}.$$

It is easy to see that this set is in Π_1^1 ; we just write out its definition carefully and then count quantifiers. The set is not in Σ_1^1 ; in fact by a classical result it is not even analytic.

11. Recursive analogues of classical objects

The recursive functions are those you can actually write computer programs for; the others are more slippery and elusive. If one wants to approach mathematics from a constructive viewpoint, the recursive functions have a firmer ontological status than the others. One can, in principle, approach a mathematical object (the set of countable ordinals and the set of real numbers will be featured examples), and extract that part of it that is sufficiently constructive to be treated by recursion theory. This constructive part can then be viewed as a recursive analogue of the original.

As a preliminary example, let us consider the extent to which the collection R of total recursive functions on $\mathbb{N}$ is an analogue for the collection $\mathbb{N}^{\mathbb{N}}$ of all functions on $\mathbb{N}$. There is the obvious disparity of size; $\mathbb{N}^{\mathbb{N}}$ is uncountable whereas there are only countably many recursive functions. But the complete analogue of the uncountability of $\mathbb{N}^{\mathbb{N}}$ would say that there is no recursive one-to-one correspondence between the natural numbers and indices of total recursive functions. One formulation of this phenomenon is the following simple result.

11.1. THEOREM. *There is no total recursive function f on $\mathbb{N}$ such that $\{\{f(n)\}: n \in \mathbb{N}\}$ coincides with the collection R of total recursive functions.*

PROOF. As in the proof of the uncountability of $\mathbb{N}^{\mathbb{N}}$, we diagonalize. The equation $g(x) = \{f(x)\}(x) + 1$ defines a total recursive function that f has omitted. There is another proof that gives more quantitative information. From the fact (see Section 10) that R is not Π_3 , we conclude that there cannot be any Σ_2 set A such that $R = \{\{x\}: x \in A\}$. $\square$

The operations of addition, multiplication, and composition of functions are applicable to R as well as to $\mathbb{N}^{\mathbb{N}}$. But from the recursive viewpoint we need additional information: it must be possible, given indices of f and g , to find effectively indices for $f + g$, $f \cdot g$, and $f \circ g$. To prove that this can indeed be done, observe for example that $\{x\}(z) + \{y\}(z)$ is a recursive partial function of x, y , and z , and apply the parameter theorem.

We can summarize this by saying that the operations of addition, multiplication, and composition of functions are “effective on the indices”. That is, each of our functions has indices that denote it, and operations on the functions are induced by operations on the indices, which in the present case are recursive operations. This phenomenon will recur in the subsequent examples: the constructive members of the classical object come with indices that denote them, and effective operations must work with these names.

For a more serious example of a recursive analogue of a classical object, take (as a classical object) the set of countable ordinals. Knowing that ordinal numbers are useful in transfinite constructions (as in the Borel hierarchy), we should not be surprised to find that a recursive analogue would be useful in transfinite constructions in recursion theory (as in the hyperarithmetical hierarchy, mentioned in the preceding section).

A cheap analogue is provided by the set

$$W = \{x: \{x\}^{2,0} \text{ encodes a well ordering}\},$$

where f is said to encode a well ordering if f is a total function from $\mathbb{N} \times \mathbb{N}$ into $\{0, 1\}$ and $\{(x, y): f(x, y) = 0\}$ is a well ordering of a subset of $\mathbb{N}$. More briefly, we can refer to W as the set of indices of recursive well orderings. For x in W , let $\|x\|$ be the ordinal number of the corresponding well ordering. Since an initial segment of a recursive well ordering is another such ordering, the set $\{\|x\|: x \in W\}$ is an initial segment of the countable ordinals. Its least upper bound will be called "recursive ω_1 ". Although recursive ω_1 is countable, it is the first ordinal that is not recursively countable.

Unfortunately, W has some deficiencies that impair its usefulness. For example, given x in W , we cannot tell effectively whether $\|x\|$ is a successor ordinal. Even if it is a successor ordinal, we cannot effectively find a member of W denoting the predecessor.

A better quality analogue is provided by a system of ordinal notations introduced by KLEENE [1938]. The set O is built up from below, unlike the set W . We will give an inductive definition simultaneously for the set O , the binary relation $<_o$, and a map $x \mapsto |x|$ from O into the ordinals. (The definition differs only slightly from Kleene's version.)

(i) $1 \in O$ and $|1| = 0$. Thus 1 is the unique number denoting the ordinal 0.

(ii) If $x \in O$ then $2^x \in O$, $x <_o 2^x$, and $|2^x| = |x| + 1$. This is the successor step.

(iii) If $x <_o y <_o z$ then $x <_o z$. The relation $<_o$ will in the end be a partial well ordering on O .

(iv) If $\{e\}$ is a total recursive increasing sequence of notations (i.e., $\{e\}: \mathbb{N} \rightarrow O$ and $\{e\}(n) <_o \{e\}(n+1)$ for each n), then $3 \cdot 5^e \in O$, $\{e\}(n) <_o 3 \cdot 5^e$ for each n , and $|3 \cdot 5^e| = \sup\{|\{e\}(n)|: n \in \mathbb{N}\}$.

This inductive definition assigns notations to an initial segment $\{|x|: x \in O\}$ of the countable ordinals. It turns out that the least ordinal not receiving a notation is again recursive ω_1 . In fact there are several other ways to characterize recursive ω_1 : it is the least ordinal that is not the order type of any Σ^1_1 well ordering of numbers, and it is the least admissible ordinal after ω (in the sense of Chapter C.5).

As a final example of recursive analogues, we will consider recursive real numbers. This subject was first treated in TURING [1936]; a more recent reference is RICE [1954]. Any real number can be approximated by rationals, but we want to single out those numbers for which we can effectively generate rational approximations, and with a known estimate of the error. These are the realiest of the reals.

Just as there are several ways to construct the reals from the rationals, so

are there several equivalent ways of making precise the concept of a recursive real. For example, we could require that the binary expansion of the fractional part of the number be given by a recursive function. Equivalently, we can adapt the Cauchy sequence construction. To each natural number n assign the rational number $r(n) = ((n)_0 - (n)_1)/((n)_2 + 1)$. Then say that e denotes a recursive real if $\{e\}$ is total and whenever $m > n$ then

$$|r(\{e\}(n)) - r(\{e\}(m))| < \frac{1}{2^n}.$$

The essential feature of both definitions is that we can effectively produce both upper and lower rational bounds converging to the number.

The recursive reals form a field, since for $x \neq 0$ we can get rational bounds of the same sign which then convert to rational bounds on $1/x$. (But given that e denotes a recursive real, there is no effective way to decide whether that real is zero.) Not only do we get a field, but the algebraic operations are "effective on the indices", e.g., there is a recursive function f such that if a and b denote recursive reals then $f(a, b)$ denotes their sum.

The algebraic real numbers are all recursive. In fact it is not too hard to see that the recursive reals form a real closed ordered field, i.e., an ordered field in which any polynomial that changes sign has an intervening root. Consequently the result of adjoining $\sqrt{-1}$ to the field is algebraically closed. (See VANDER WAERDEN [1953], section 70.) Furthermore by Tarski's theorem, the field of recursive reals is elementarily equivalent to the field of all real numbers (see Chapter A.2).

In addition to the algebraic numbers, various transcendental numbers such as e and π are recursive, since there are well-known methods of churning out convergent upper and lower rational bounds.

The recursive reals are not as kind to analysts as they are to algebraists. The following example occurs in RICE [1954]; see also SPECKER [1949]. Start with a non-recursive r.e. set K . There is a one-to-one total recursive function f whose range is K (think of $f(n)$ as the $(n+1)$ -st distinct number to emerge in an effective enumeration of K). Consider the set of rational numbers:

$$\frac{1}{2^{f(0)}}, \quad \frac{1}{2^{f(0)}} + \frac{1}{2^{f(1)}}, \quad \frac{1}{2^{f(0)}} + \frac{1}{2^{f(1)}} + \frac{1}{2^{f(2)}}, \quad \dots$$

This is a bounded recursive set of rational numbers. But its least upper bound (which is the only limit point of the set) is not a recursive real number, lest K be recursive.

Finally, let us consider the analogues of functions of a real variable. A function F from the set of recursive reals into itself is called a *recursive*

operator if there is a recursive partial function f such that whenever e denotes a recursive real x then $f(e)$ is defined and denotes $F(x)$. Thus f , working on the indices, performs F . We state without proof the following result.

11.2. THEOREM (KREISEL, LACOMBE and SHOENFIELD [1959], CEĬTIN [1959]). *Every recursive operator is continuous. Moreover, given an e denoting a recursive real and a positive rational ε , we can effectively find a δ that works.*

References

- BLUM, M.
[1967] A machine-independent theory of the complexity of recursive functions, *J. Assoc. Comput. Mach.*, **14**, 322–336.
- BRADY, A.H.
[1966] The conjectured highest scoring machines for Rado's $\Sigma(k)$ for the value $k = 4$, *IEEE Trans. Computers*, EC-15, 802–803.
[1975] The solution to Rado's "busy beaver game" is now decided for $k = 4$ (abstract), *Notices Am. Math. Soc.*, **22**, A–25.
- CEĬTIN, G.S.
[1959] Algorithmic operators in constructive complete separable metric spaces (Russian), *Dokl. Akad. Nauk SSSR*, **128**, 49–52.
- CHURCH, A.
[1935] An unsolvable problem of elementary number theory (abstract), *Bull. Am. Math. Soc.*, **41**, 332–333.
[1936] An unsolvable problem of elementary number theory, *Am. J. Math.*, **58**, 345–363.
- DAVIS, M.
[1958] *Computability and Unsolvability* (McGraw-Hill, New York).
- FEFERMAN, S.
[1957] Degrees of unsolvability associated with formalized theories, *J. Symbolic Logic*, **22**, 161–175.
- FRIEDBERG, R.M.
[1957] Two recursively enumerable sets of incomparable degrees of unsolvability (solution of Post's problem, 1944), *Proc. Nat. Acad. Sci. U.S.A.*, **43**, 236–238.
- GÖDEL, K.
[1931] Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. *Monatsh. Math. Phys.*, **38**, 173–198.
[1965] On undecidable propositions of formal mathematical systems, in: *The Undecidable, Basic Papers on Undecidable Propositions, Unsolvability Problems and Computable Functions* (Raven Press, Hewlett, NY) pp. 41–71.
- GREEN, M.W.
[1964] A lower bound on Rado's sigma function for binary Turing machines, in: *Switching Circuit Theory and Logical Design*, Proceedings of the fifth annual symposium, The Institute of Electrical and Electronics Engineers, pp. 91–94.
- HANF, W.
[1965] Model-theoretic methods in the study of elementary logic, in: *The Theory of Models*, Proceedings of the 1963 international symposium at Berkeley (North-Holland, Amsterdam) pp. 132–145.

KAHR, A.S., MOORE, E.F. and WANG, H.

- [1962] Entscheidungsproblem reduced to the $\forall\exists\forall$ case, *Proc. Nat. Acad. Sci, U.S.A.*, **48**, 365–377.

KLEENE, S.C.

- [1936a] General recursive functions of natural numbers, *Math. Ann.*, **112**, 727–742.
 [1936b] λ -definability and recursiveness, *Duke Math. J.*, **2**, 340–353.
 [1938] On notation for ordinal numbers, *J. Symbolic Logic*, **3**, 150–155.
 [1943] Recursive predicates and quantifiers, *Trans. Am. Math. Soc.*, **53**, 41–73.
 [1952] *Introduction to Metamathematics* (North-Holland, Amsterdam; 7-th reprint, 1974).

KREISEL, G., LACOMBE, D. and SHOENFIELD, J.R.

- [1957] Partial recursive functionals and effective operations, in: *Constructivity in Mathematics*, Proceedings of the colloquium held at Amsterdam, 1957 (North-Holland, Amsterdam) pp. 290–297.

LIN, S. and RADO, T.

- [1965] Computer studies of Turing machine problems, *J. Assoc. Comput. Mach.*, **12**, 196–212.

MATIJACEVIČ, YU. V.

- [1970] Recursively enumerable sets are Diophantine (Russian), *Dokl. Akad. Nauk SSSR*, **191**, 279–282.

MUČNIK, A.A.

- [1956] Negative answer to the problem of reducibility in the theory of algorithms (Russian), *Dokl. Akad. Nauk SSSR*, **108**, 194–197.

MYHILL, J.

- [1955] Creative sets, *Z. Math. Logik Grundlagen Math.* **1**, 97–108.

POST, E.L.

- [1936] Finite combinatory processes—formulation I. *J. Symbolic Logic*, **1**, 103–105.
 [1944] Recursively enumerable sets of positive integers and their decision problems, *Bull. Am. Math. Soc.*, **50**, 284–316.
 [1948] Degrees of recursive unsolvability (abstract). *Bull. Am. Math. Soc.*, **54**, 641–642.

RABIN, M.O.

- [1960] Degree of difficulty of computing a function and a partial ordering of recursive sets, technical report No. 2, Hebrew University, Jerusalem.

RADO, T.

- [1962] On non-computable functions. *Bell System Tech. J.*, **41**, 877–884.

RICE, H.G.

- [1953] Classes of recursively enumerable sets and their decision problems, *Trans. Am. Math. Soc.*, **74**, 358–366.
 [1954] Recursive real numbers, *Proc. Am. Math. Soc.*, **5**, 784–791.

ROGERS, H. JR.

- [1967] *Theory of Recursive Functions and Effective Computability* (McGraw-Hill, New York).

SACKS, G.E.

- [1963] *Degrees of Unsolvability* (Princeton University Press, Princeton, NJ).
 [1964] The recursively enumerable degrees are dense, *Ann. of Math.*, **80**, 300–312.

SHOENFIELD, J.R.

- [1958] The class of recursive functions, *Proc. Am. Math. Soc.*, **9**, 690–692.
 [1962] The form of the negation of a predicate, in: *Recursive Function Theory*, edited by J. Dekker, Proceedings of symposia in pure mathematics, Vol. 5 (Am. Math. Soc., Providence, RI) pp. 131–134.
 [1967] *Mathematical Logic* (Addison-Wesley, Reading, MA).
 [1971] *Degrees of Unsolvability* (North-Holland, Amsterdam).

SOUSLIN, M.

- [1917] Sur une définition des ensembles mesurables B sans nombres transfinis, *C.R. Acad. Sci. Paris*, **164**, 88–91.

SPECKER, E.

- [1949] Nicht konstruktiv beweisbare Sätze der Analysis, *J. Symbolic Logic*, **14**, 145–158.

TURING, A.M.

- [1936] On computable numbers, with an application to the Entscheidungsproblem, *Proc. London Math. Soc.*, Ser. 2, **42**, 230–265.

- [1939] Systems of logic based on ordinals, *Proc. London Math. Soc.*, Ser. 2, **45**, 161–228.

VAN DER WAERDEN, B.L.

- [1953] *Modern Algebra*, Vol. 1 (Frederick Ungar, New York, revised English ed.).

YASUHARA, A.

- [1971] *Recursive Function Theory and Logic* (Academic Press, New York).

Unsolvable Problems

MARTIN DAVIS*

Contents

Introduction	568
1. The halting problem revisited	569
2. Semi-Thue processes	571
3. Semigroups and groups	575
4. Other combinatorial problems	580
5. Diophantine equations	584
References	592

* Work supported by National Science Foundation Grant DCR 71-02039 A05.

Introduction

Many important mathematical problems take the form: find an algorithm (i.e. an effective procedure) by means of which it can be determined (in a finite number of steps) for each element of a given set, whether or not the element possesses some given property. The “solution” of such a “decision” problem is then to consist of actually exhibiting an algorithm and providing a proof that the algorithm does what is required of it.

A standard example from the elementary theory of numbers is to give an algorithm by means of which it can be determined for a given ordered triple $\langle a, b, c \rangle$ of integers, whether or not the equation

$$ax + by = c$$

has a solution in integers. In this case, a solution is: find the largest natural number d which simultaneously divides a and b and then test whether or not d is a divisor of c . (The equation will have an integer solution just in case d does divide c .) Now, the development of recursion theory with its precise explication of the intuitive notion of effective computability has made a new alternative available: instead of solving a decision problem positively by showing the existence of an algorithm, we can solve it negatively by proving that no algorithm meeting the requirements exists. Or, as we say, we can prove that the problem is *unsolvable*. Thus, Hilbert’s tenth problem, which sought an algorithm for testing an arbitrary polynomial equation $P(x_1, \dots, x_n) = 0$ with integer coefficients for possessing a solution in integers, was shown to be unsolvable by MATIJACEVIČ [1970].

The only prerequisite for this chapter is familiarity with Sections 1–4 of Chapter C.1, *Elements of recursion theory*, which we cite as ERT and whose notation we follow. We shall survey the main unsolvability results which have been obtained for problems of genuine mathematical interest. In some cases we shall give complete proofs, in others we shall content ourselves with an outline of the main ideas.

The mathematical content of an unsolvability result is that some particular set is not recursive. And in fact, if S is any non-recursive set of natural numbers, we can assert the unsolvability of the decision problem: *to determine of a given $x \in \mathbb{N}$ whether or not $x \in S$* . Of course this conclusion is based on the identification of the intuitive notion “ S is decidable” with the precise notion “ S is recursive”, i.e. what is usually called Church’s thesis. (Cf. Section 3 of ERT.) In this chapter we freely use Church’s thesis often without specific comment. As just indicated this is necessary if we are to conclude from the non-recursiveness of a set, that there really is no

corresponding algorithm. But in addition it will be used to simplify proofs: whenever we exhibit an algorithm for computing the values of a partial function f we will conclude without further ado that f is a recursive partial function.

In addition to proving that certain mathematical decision problems are unsolvable, there has been considerable interest in calculations of the *degree of unsolvability* of such problems in the sense discussed in ERT, Section 8. However, we shall not discuss these matters in this chapter.

1. The halting problem revisited

The unsolvability of the halting problem is given in 4.2 of ERT in the form:

The set $K = \{x: \{x\}(x) < \infty\}$ is not recursive.

By the Normal Form Theorem (ERT, 4.1), $\{x\}(x)$ is a recursive partial function of x . Hence by the discussion of Section 2 of ERT, there is some Turing machine M (which could in fact be concretely exhibited at the cost of some unpleasant labor) such that:

If we start M at instruction q_0 scanning the leftmost symbol of $\ulcorner x \urcorner$ (with all the remaining symbols on the tape blank), then M eventually halts if and only if $\{x\}(x)$ is defined, i.e. if and only if $x \in K$. In the rest of this chapter, M will always stand for this Turing machine.

Since K is not recursive we conclude:

1.1. THEOREM. *There is no algorithm for testing a given $x \in \mathbb{N}$ to determine whether or not M will eventually halt when started at instruction q_0 scanning the leftmost symbol of $\ulcorner x \urcorner$.*

By weakening this result it assumes a more elegant form (recall from ERT, Section 4 that a *configuration* for a Turing machine consists of the current contents of the machine tape, the instruction number, and the square being scanned):

1.2. COROLLARY. *There is no algorithm for testing a given configuration of M to determine whether or not M will eventually halt when started at the given configuration.*

Of course the machine M is formally a function (as explained in

Definition 2.1 of ERT) which can be concretely exhibited as a table with five columns and an appropriate number of rows, or as we shall say, *quintuples*. (Cf. the example in Section 2 of ERT of a Turing machine which computes $x + y$.) The halting problem for M is then a quite specific mathematical question: for which of a given set of configurations will a certain well-defined combinatorial process eventually terminate?

The halting problem will play a fundamental role in this article. Indeed the unsolvability of all the problems which we will discuss follows from that of the halting problem.

1.3. DEFINITION. A k -ary relation R on $\mathbb{N}$ is *recursively enumerable* (abbreviated r.e.) if there is a Turing machine T such that whenever we start T at instruction q_0 scanning the leftmost symbol of

$$\lceil x_1 \rceil 0 \lceil x_2 \rceil 0 \cdots 0 \lceil x_k \rceil$$

(with the rest of the tape blank), then T eventually halts if and only if $\langle x_1, \dots, x_k \rangle \in R$.

Recursive enumerability of a k -ary relation on N is defined in Section 6 of ERT (which is beyond our formal prerequisites) in a slightly different, but equivalent, way. The equivalence proof requires overcoming a not very profound technical hurdle. Of course we will use the present definition throughout this chapter.

Intuitively, to say that R is r.e. is to say that we possess an algorithm which will ultimately find any correct "yes" answers to questions of the form "Is it the case that $\langle x_1, \dots, x_k \rangle \in R$?" but will fail to terminate when the answer is "no".

Writing $\bar{R}$ for the *complement* of the k -ary relation R (i.e. $\langle x_1, \dots, x_k \rangle \in \bar{R}$ if and only if $\langle x_1, \dots, x_k \rangle \notin R$), we have:

1.4. THEOREM. R is recursive if and only if R and $\bar{R}$ are r.e.

PROOF. Let R be recursive and let its characteristic function (i.e. the function which is 1 when R is true and 0 when it is false) be computed by Turing machine M_0 . Let $q_0, q_1, \dots, q_n$ be the instructions of M_0 . We modify M_0 to obtain new machines M^+ and M^- by adjoining additional states and quintuples. For each pair (i, α) , $0 \leq i \leq n$, $\alpha = 0$ or 1 , for which M_0 's table contains no quintuple beginning i, α (i.e. M_0 will halt at once if it comes to instruction q_i scanning a square on which α is written), we place in the tables of both M^+ and M^- the quintuples:

$$i \alpha \quad \alpha R (n + 1).$$

Now, when M_0 halts, the scanned square contains 1, and its right-hand neighbor contains 1 if R is true for the given inputs, and 0 if R is false for the given inputs. Thus, on arriving at instruction $n + 1$, M^+ and M^- find themselves scanning 1 or 0 according as R is true or false for the given inputs. Finally, we add to M^+ the quintuple

$$(n + 1)0 \quad 0 \quad R \quad (n + 1)$$

and to M^- the quintuples

$$(n + 1)1 \quad 1 \quad R \quad (n + 2)$$

$$(n + 2)0 \quad 0 \quad R \quad (n + 2).$$

Then M^+ halts for given $\langle x_1 \rangle 0 \cdots 0 \langle x_k \rangle$ if and only if $\langle x_1, \dots, x_k \rangle \in R$ and M^- halts if and only if $\langle x_1, \dots, x_k \rangle \in \bar{R}$.

Conversely, if R and $\bar{R}$ are r.e. we are given Turing machines M^+ , M^- which halt on given $\langle x_1 \rangle 0 \cdots 0 \langle x_k \rangle$ in case $\langle x_1, \dots, x_k \rangle \in R$ or $\notin R$ respectively. Thus, to test whether or not $\langle x_1, \dots, x_k \rangle \in R$ for given $x_1, \dots, x_k$ we need only run M^+ , M^- simultaneously until one of them halts. So, R is intuitively decidable, and, using Church's thesis, it is recursive.

Since the machine M used in our discussion of the halting problem eventually halts for given x if and only if $x \in K$ we have:

1.5. THEOREM. *The set K is r.e. but not recursive. Hence $\bar{K}$ is not r.e.*

2. Semi-Thue processes

Let $A = \{a_1, \dots, a_k\}$ be some given finite set of objects we call *symbols*. A is then called an *alphabet*, and a finite sequence of elements of A is called a *string* or a *word* on A . The basic operation on strings is *concatenation*. That is, if $u = a_{i_1}a_{i_2} \cdots a_{i_k}$, $v = a_{j_1}a_{j_2} \cdots a_{j_l}$ are strings on A , we write

$$uv = a_{i_1}a_{i_2} \cdots a_{i_k}a_{j_1}a_{j_2} \cdots a_{j_l}.$$

Note that $u(vw) = (uv)w$. It is convenient to permit the *null string* Λ of length 0 where $u\Lambda = \Lambda = u$, for all strings u .

2.1. DEFINITION. A *semi-Thue production* (on A) (or just *production*) is an ordered pair $\langle g, \bar{g} \rangle$ of words on A . It is customary to write the production in the form: $g \rightarrow \bar{g}$. A *semi-Thue process* (on A) is a finite non-empty set of semi-Thue productions on A .

2.2. DEFINITION. Let P be the semi-Thue production $g \rightarrow \bar{g}$. Then we write $u \Rightarrow_P v$ (omitting the P when there is no ambiguity) if we have $u = agb$ and $v = a\bar{g}b$ for (possibly null) strings a, b .

2.3. DEFINITION. Let Π be a semi-Thue process. Then we write $u \Rightarrow_{\Pi} v$ if $u \Rightarrow_P v$ for some $P \in \Pi$. We write $u \Rightarrow_{\Pi}^* v$ if there is a finite sequence: $u = u_1 \Rightarrow_{\Pi} u_2 \Rightarrow_{\Pi} \cdots \Rightarrow_{\Pi} u_n = v$, for $n \geq 1$. (In particular $u \Rightarrow_{\Pi}^* u$.) Again, we omit the Π when no ambiguity will result. (In displays the symbols P or Π are set directly below the $\Rightarrow$ and the $*$ directly above it.)

The *word problem* for a given semi-Thue process Π is the decision problem: *to find an algorithm by means of which it can be determined for given words u, v whether or not $u \Rightarrow^* v$.*

We shall see that there are semi-Thue systems whose word problem is unsolvable. In fact we shall show how to obtain from any given Turing machine T , a corresponding semi-Thue system $\Pi(T)$ such that an algorithm for solving the word problem for $\Pi(T)$ can also be used to solve the halting problem for T . Together with the results of Section 1, this will yield the desired result.

Thus let T be a Turing machine with instructions $q_0, q_1, \dots, q_n$. Then, $\Pi(T)$ will be a semi-Thue process on the alphabet:

$$A = \{0, 1, q_0, q_1, \dots, q_n, q, q', h\}.$$

The successive configurations of T through the course of a computation will each be represented by a so-called *Post word*, that is a word on A of the form:

$$h u q_i v h \quad (1)$$

where u, v are words on $\{0, 1\}$, $v \neq \Lambda$, and $0 \leq i \leq n$. Here the Post word (1) is to represent a configuration in which q_i is the current instruction, the tape contents is uv (augmented by infinite sequences of 0's on its left and right) and the initial symbol of v is being scanned. The h 's serve as punctuation marks; their importance will soon be plain. Since it is not precluded that u begin with 0 or that v end with 0, there are infinitely many different Post words corresponding to a given configuration of T . The effect of T on successive configurations will be mimicked (or as is sometimes said, *simulated*) by productions of $\Pi(T)$ which will have corresponding effects on the Post words.

In fact, the productions of $\Pi(T)$ are as follows:

(i) For each quintuple in the table of T of the form

$$i \alpha \quad \beta R j \quad \alpha, \beta \in \{0, 1\}$$

$\Pi(T)$ is to contain the three productions

$$q_i \alpha 0 \rightarrow \beta q_i 0$$

$$q_i \alpha 1 \rightarrow \beta q_i 1$$

$$q_i \alpha h \rightarrow \beta q_i 0 h.$$

(ii) For each quintuple in the table of T of the form

$$i \alpha \quad \beta L j \quad \alpha, \beta \in \{0, 1\},$$

$\Pi(T)$ is to contain the three productions

$$0 q_i \alpha \rightarrow q_i 0 \beta$$

$$1 q_i \alpha \rightarrow q_i 1 \beta$$

$$h q_i \alpha \rightarrow h q_i 0 \beta.$$

(iii) For each pair $\langle i, \alpha \rangle$, $0 \leq i \leq n$, $\alpha \in \{0, 1\}$ for which no quintuple in the table of T begins $i \alpha$, $\Pi(T)$ is to contain the production

$$q_i \alpha \rightarrow q \alpha.$$

(iv) Finally $\Pi(T)$ contains the five productions:

$$q 0 \rightarrow q$$

$$q 1 \rightarrow q$$

$$q h \rightarrow q' h$$

$$0 q' \rightarrow q'$$

$$1 q' \rightarrow q'.$$

Now suppose that $h u q_i \alpha \gamma v h$, where $\alpha, \gamma \in \{0, 1\}$ is a Post word which corresponds to a given configuration of T and that the table of T contains the quintuple

$$i \alpha \quad \beta R j.$$

Then we have

$$h u q_i \alpha \gamma v h \xRightarrow{\Pi(T)} h u \beta q_i \gamma v h$$

and in fact $h u \alpha q_i \gamma v h$ is a Post word corresponding to the next configuration T . (I.e. α has been replaced by β on the tape, the scanned square has been moved one to the right, and instruction q_i is the new current instruction.) In the case where the Post word has the form $h u q_i \alpha h$, we have:

$$h u q_i \alpha h \xRightarrow{\Pi(T)} h u \beta q_i 0 h,$$

i.e. the necessary blank has been appended on the right by the unique production which can be applied. Thus the total effect of the productions listed under (i) is to cause changes in a Post word exactly corresponding to the effect on a machine configuration of the quintuple: $i \alpha \beta R j$. It is easy to check that the productions listed under (ii) behave analogously for quintuples of the form: $i \alpha \beta L j$.

The productions listed under (iii) will be able to operate on a Post word just in case it corresponds to a configuration of T in which T has just been forced to halt. The effect is to replace the instruction symbol q_i by q . Finally, if u, v are words on $\{0, 1\}$, we have with respect to the productions of (iv):

$$h u q v h \xRightarrow{*} h u q h \xRightarrow{*} h u q' h \xRightarrow{*} h q' h. \quad (2)$$

Now let T begin at instruction q_0 scanning the leftmost symbol of $^1x^1$ (with the rest of the tape blank). The corresponding Post word is $h q_0 ^1x^1 h$. First suppose that T will eventually halt. Then by the above discussion (in particular noting (2)), we have:

$$h q_0 ^1x^1 h \xRightarrow{\Pi(T)} h u q v h \xRightarrow{\Pi(T)} h q' h.$$

Conversely, if

$$h q_0 ^1x^1 h \xRightarrow{\Pi(T)} h q' h,$$

then in the sequence

$$h q_0 ^1x^1 h = u_1 \Rightarrow u_2 \Rightarrow \cdots \Rightarrow u_n = h q' h,$$

each u_i must contain exactly one q -symbol (the q -symbols are of course $q_0, q_1, \dots, q_n, q, q'$), since each production preserves this property. The productions of (i), (ii) each replaces some q_i by a q_j , those of (iv) can never replace a q_i . Hence a production from (iii) must have been used at least (and therefore exactly) once. But this implies that T eventually halts. We have proved:

2.4. THEOREM. *The Turing machine T beginning at instruction q_0 scanning the leftmost symbol of $^1x^1$ (with the rest of the tape blank) will eventually halt if and only if:*

$$h q_0 \text{ 'x' } h \xRightarrow[\Pi(T)]{*} h q' h.$$

Setting $T = M$ and using Theorem 1.1, we have at once:

2.5. COROLLARY. *There is no algorithm for testing a given $x \in \mathbb{N}$ to determine whether or not*

$$h q_0 \text{ 'x' } h \xRightarrow[\Pi(M)]{*} h q' h.$$

In particular:

2.6. COROLLARY. *The word problem for $\Pi(M)$ is unsolvable.*

We conclude this section with a technical observation about $\Pi(T)$ which we will find useful in the next section:

2.7. REMARK. If u is a word on the alphabet of A containing exactly one q -symbol, then there is at most one production $P \in \Pi(T)$ such that $u \Rightarrow_P v$ for some word v .

The remark simply reflects the fact that no two quintuples beginning with the same pair $i\alpha$ can be part of the table of a Turing machine.

3. Semigroups and groups

We have already remarked that the operation of concatenation of strings on the alphabet $A = \{a_1, \dots, a_k\}$ is associative. In algebraic language, this fact is expressed by saying that the set of strings forms a *semigroup* under concatenation.

3.1. DEFINITION. The *inverse* of the semi-Thue production $g \rightarrow \bar{g}$ is the production $\bar{g} \rightarrow g$. A semi-Thue process Π is called a *Thue process* if for each $P \in \Pi$, the inverse of P is also in Π .

For any semi-Thue process Π , the relation $u \Rightarrow_{\Pi}^* v$ is obviously reflexive and transitive. If Π is a *Thue process*, then whenever

$$u = u_1 \xRightarrow[\Pi]{} u_2 \xRightarrow[\Pi]{} \dots \xRightarrow[\Pi]{} u_n = v, \quad (3)$$

clearly

$$v = u_n \xRightarrow[\Pi]{} u_{n-1} \xRightarrow[\Pi]{} \cdots \xRightarrow[\Pi]{} u_1 = u,$$

so that the relation $u \xRightarrow[\Pi]{}^* v$ is also symmetric, and hence is an equivalence relation, which we write $u \sim_{\Pi} v$. We write $[u]$ for the equivalence class containing u . It is also clear that whenever (3) holds, we have for all words w on A

$$w u = w u_1 \xRightarrow[\Pi]{} w u_2 \xRightarrow[\Pi]{} \cdots \xRightarrow[\Pi]{} w u_n = w v$$

and

$$u w = u_1 w \xRightarrow[\Pi]{} u_2 w \xRightarrow[\Pi]{} \cdots \xRightarrow[\Pi]{} u_n w = v w.$$

Hence, if $u \sim_{\Pi} v$ and $u' \sim_{\Pi} v'$ we have

$$u u' \sim_{\Pi} v u' \sim_{\Pi} v v'.$$

Thus, writing

$$[u] \cdot [u'] = [u u'],$$

this product is well defined, and since the operation is associative, the resulting structure is a semigroup.

If S is a semigroup defined in this way, the Thue process Π is called a *presentation* of S . Each pair $\langle g, \bar{g} \rangle$ such that $g \rightarrow \bar{g}$ (and hence also $\bar{g} \rightarrow g$) is a production of Π , is called a *relation* of the presentation, and is usually written $g \sim \bar{g}$ (or even $g = \bar{g}$). Finally the symbols belonging to A are called the *generators* of the presentation. Of course a given abstract semigroup may well have many different presentations (or indeed none at all).

If Π is a semi-Thue process, we write $\bar{\Pi}$ for the Thue process obtained from Π by adjoining to it the inverse of each production of Π . We have

3.2. LEMMA (POST [1947]). *For any Turing machine T and $x \in N$, we have :*

$$h q_0 \ulcorner x \urcorner h \xRightarrow[\Pi(T)]{}^* h q' h$$

if and only if

$$h q_0 \ulcorner x \urcorner h \sim_{\bar{\Pi}(T)} h q' h.$$

PROOF Since $\Pi(T) \subseteq \bar{\Pi}(T)$ the lemma is obvious in one direction.

Conversely, let

$$h q_0 {}^{\lceil x \rceil} h = u_1 \xRightarrow[\Pi(T)]{} u_2 \xRightarrow[\Pi(T)]{} \cdots \xRightarrow[\Pi(T)]{} u_n = h q' h.$$

Suppose furthermore that

$$u_1 \xRightarrow{P_1} u_2 \xRightarrow{P_2} \cdots \xRightarrow{P_{i-1}} u_i \xRightarrow{P_i} u_{i+1} \xRightarrow{P_{i+1}} u_{i+2} \cdots \xRightarrow{P_{n-1}} u_n$$

where $P_{i+1}, \dots, P_{n-1} \in \Pi(T)$ but $P_i \notin \Pi(T)$. Since no production of $\Pi(T)$ can apply to $h q' h$, no inverse of such a production can yield $h q' h$ as a result; i.e. $i < n - 1$. It is clear that the words $u_1, \dots, u_n$ each contain exactly one q -symbol, since the productions of $\bar{\Pi}(T)$ preserve this property. Let Q be the inverse of P_i so that $Q \in \Pi(T)$ and $u_{i+1} \xRightarrow{Q} u_i$. Since also $u_{i+1} \xRightarrow{P_{i+1}} u_{i+2}$ and $P_{i+1} \in \Pi(T)$, Remark 2.7 implies that $u_i = u_{i+2}$. Hence we have

$$u_1 \xRightarrow{P_1} u_2 \xRightarrow{P_2} \cdots \xRightarrow{P_{i-1}} u_i \xRightarrow{P_{i+2}} u_{i+3} \cdots \xRightarrow{P_{n-1}} u_n$$

and the production P_i has been eliminated. Repeating the process, all productions which do not belong to $\Pi(T)$ can be eliminated, yielding the desired conclusion. $\square$

Referring to the corollaries 2.5 and 2.6, we have:

3.3. COROLLARY (POST [1947]). *There is no algorithm for testing a given $x \in N$ to determine whether or not*

$$h q_0 {}^{\lceil x \rceil} h \sim_{\Pi(M)} h q' h.$$

3.4. COROLLARY (POST [1947], MARKOV [1949]). *There is a presentation of a semigroup with an unsolvable word problem.*

The word problem for semigroups was first considered by THUE [1914] long before the development of recursion theory raised the possibility of a negative solution. It was historically the first example of a decision problem whose original formulation was in no way related to logic and for which an unsolvability proof was given.

We now turn to an important special case of semigroup presentations: Let A contain an even number of symbols:

$$A = \{a_1, \dots, a_k, b_1, \dots, b_k\}$$

and let the relations of the Thue process Π contain all relations

$$a_i b_i \sim \Lambda, \quad i = 1, 2, \dots, k.$$

(Of course, in general, Π will contain other relations as well.) In this case Π is called a *group presentation* and (as is readily verified) it is indeed a presentation of a *group*. An abstract group G which has a group presentation is said to be *finitely presented*. Because of its importance in algebraic topology particular attention has been paid to the word problem for group presentations (or as one says: *the word problem for groups*). The Novikov–Boone theorem which asserts the existence of a group presentation with an unsolvable word problem thus represented a major breakthrough. Unfortunately, space does not permit our giving a proof of this theorem here. We refer the interested reader to BOONE [1959] (which is based on the construction of $\bar{\Pi}(M)$), NOVIKOV [1955], BRITTON [1963], ROTMAN [1973], Chapter 12, and to MCKENZIE and THOMPSON [1973]. The last paper referred to is in BOONE, CANNONITO and LYNDON [1973] which contains a wealth of interesting material and references in this area.

3.5. DEFINITION. We say that an abstract group G is *recursively presented* if there are elements $c_1, \dots, c_n \in G$ such that:

(i) each element of G can be written in the form $c_1^{m_1} \cdots c_n^{m_n}$ where $m_1, \dots, m_n \in \mathbb{Z}$ (here $\mathbb{Z}$ is the set of integers positive, negative, and 0), i.e., $c_1, \dots, c_n$ generate the group G ;

(ii) the relation $R = \{\langle m_1, \dots, m_n \rangle \mid c_1^{m_1} \cdots c_n^{m_n} = e\}$, where e is the identity element of G is recursively enumerable.

Of course there is no difficulty in speaking of r.e. relations on $\mathbb{Z}$ rather than $\mathbb{N}$. E.g. we can set $\bar{m} = 2m$ if $m \geq 0$ and $\bar{m} = -2m - 1$ if $m < 0$ and say that for R to be r.e. means that $\{\langle \bar{m}_1, \dots, \bar{m}_n \rangle \mid \langle m_1, \dots, m_n \rangle \in R\}$ is r.e.

The Novikov–Boone theorem is an easy consequence of:

3.6. THEOREM (HIGMAN [1961]). *A group is recursively presented if and only if it is isomorphic to a subgroup of a finitely presented group.*

This surprising theorem shows that a recursion-theoretic notion (that of being a recursively presented group) is equivalent to a purely algebraic notion. Simplified proofs of Higman's theorem can be found in SHOENFIELD [1967], Appendix, AANDERAA [1973], and ROTMAN [1973], Chapter 12.

Let us say that a class $\mathbf{G}$ of groups is:

- (i) *invariant*, if $G \in \mathbf{G}$ and H isomorphic to G implies that $H \in \mathbf{G}$;
 - (ii) *non-trivial*, if there exist finitely presented groups G, H such that $G \in \mathbf{G}$ and $H \notin \mathbf{G}$;
 - (iii) *hereditary*, if $G \in \mathbf{G}$ and H a subgroup of G implies that $H \in \mathbf{G}$.
- It has been shown that:

3.7. THEOREM (ADJAN [1955], RABIN [1958]). *Let $\mathbf{G}$ be a class of groups which is invariant, non-trivial, and hereditary. Then there is no algorithm by means of which one can determine given a group presentation, whether or not the group belongs to $\mathbf{G}$.*

As an example, let $\mathbf{G}$ consist only of the trivial group $\{e\}$. We obtain:

3.8. COROLLARY. *There is no algorithm by means of which one can tell from a group presentation, whether or not the group contains at least one element other than e .*

Other group properties to which the Adjan–Rabin theorem applies are that of being:

- (i) cyclic,
- (ii) finite,
- (iii) free,
- (iv) commutative,
- (v) solvable.

The proof of the Adjan–Rabin theorem makes use of the existence of a group presentation with an unsolvable word problem, i.e. of the Novikov–Boone theorem.

By means of a straightforward construction (HAKEN [1973]), it is possible to construct from a given group presentation of a group G a 2-dimensional simplicial complex having G as its fundamental group. Since a simplicial complex is simply connected just in case its fundamental group is trivial, i.e., consists of the identity element, we can conclude from Corollary 3.8:

3.9. COROLLARY. *There is no algorithm for testing a given 2-dimensional simplicial complex to determine whether or not it is simply connected.*

By using a much more elaborate and difficult construction, MARKOV [1958] showed how given a group presentation Π it is possible to construct for each $n \geq 4$ a pair of simplicial complexes $M_1(\Pi)$, $M_2(\Pi)$ which are n -dimensional manifolds such that $M_1(\Pi)$ and $M_2(\Pi)$ are homeomorphic if

and only if the group of which Π is a presentation is trivial. Again using Corollary 3.8, we can conclude:

3.10. THEOREM. *The homeomorphism problem for manifolds of dimension ≥ 4 is unsolvable.*

The solution of the homeomorphism problem for two-dimensional manifolds is a classical result going back to Riemann. For three-dimensional manifolds, it remains open. For further discussion of topological decision problems, cf. BOONE, HAKEN and POÉNARU [1968] and HAKEN [1973].

4. Other combinatorial problems

One of the earliest examples of an unsolvable problem of a purely combinatorial nature was given in Post [1946], the so-called *correspondence* problem. Later this problem turned out to have interesting applications to the formal theory of languages.

4.1. DEFINITION. A *Post correspondence system* consists of an alphabet A and a finite set of ordered pairs $\langle h_i, k_i \rangle$, $i = 1, \dots, m$, where a word u on A is called a *solution* of the system if for some sequence $1 \leq i_1, i_2, \dots, i_n \leq m$ (the i_j 's need not be distinct), we have

$$u = h_{i_1} h_{i_2} \cdots h_{i_n} = k_{i_1} k_{i_2} \cdots k_{i_n}.$$

Let Π be a given semi-Thue process, and let u, v be a pair of words in the alphabet of Π . We shall show how to construct from Π together with u and v a Post correspondence system which has a solution if and only if $u \Rightarrow_n^* v$. Using Corollary 2.6, we will then be able to conclude:

4.2. THEOREM. *There is no algorithm for determining of a given Post correspondence system whether or not it has a solution.*

PROOF. The proof of 4.2 given here is that of Floyd (unpublished), and is considerably simpler than Post's original proof. It can also be found in YASUHARA [1971].

We proceed with the required construction. Let Π be a semi-Thue process on the alphabet $A = \{a_1, \dots, a_n\}$, and let u, v be words on A . We shall construct a Post correspondence problem P on the alphabet

$$B = \{a_1, \dots, a_n, a'_1, \dots, a'_n, [,], *, *'\},$$

consisting of $2n + 4$ symbols. For any word w on A we write w' for the word obtained from w by placing ' after each symbol of w .

Let the productions of Π be $g_i \rightarrow \bar{g}_i$, $i = 1, 2, \dots, k$ and let us assume that included among these productions are the n "identity" productions $a_i \rightarrow a_i$, $i = 1, 2, \dots, n$. This last assumption does not restrict generality (i.e. the class of pairs $\langle r, s \rangle$ for which $r \Rightarrow_n^* s$ is in no way changed by including the identity productions). However, we may now state that $u \Rightarrow_n^* v$ if and only if we can write

$$u = u_1 \xRightarrow{\Pi} u_2 \xRightarrow{\Pi} \cdots \xRightarrow{\Pi} u_m = v$$

where m is *odd*. The Post correspondence system P on the alphabet B is then to consist of the pairs:

$$\begin{aligned} &\langle [u *, [, \langle *, *' \rangle, \langle *', * \rangle, \\ &\left. \begin{array}{l} \langle \bar{g}_j, g'_j \rangle \\ \langle \bar{g}'_j, g_j \rangle \end{array} \right\} j = 1, 2, \dots, k, \quad \langle], *'v \rangle]. \end{aligned}$$

Now, let

$$u = u_1 \xRightarrow{\Pi} u_2 \xRightarrow{\Pi} \cdots \xRightarrow{\Pi} u_m = v$$

where m is *odd*. Then the word

$$w = [u_1 * u'_2 *' u_3 * \cdots * u'_{m-1} *' u_m]$$

is a solution of P as is obvious from the two decompositions

$$\begin{aligned} w &= [u_1 * | u'_2 *' | u_3 * | \cdots |] \\ &= [| u_1 * | u'_2 *' | \cdots | *' u_m]. \end{aligned}$$

To see for example that $u'_2 *'$ corresponds to $u_1 *$ we note that we can write $u_1 = r g_j s$, $u_2 = r \bar{g}_j s$ for some $j = 1, 2, \dots, k$. Then $u'_2 = r' \bar{g}'_j s'$ and the correspondence is obvious (recalling that the productions $a_1 \rightarrow a_1, \dots, a_n \rightarrow a_n$ are present in Π).

Conversely, if $\bar{w}$ is a solution, then to avoid mismatches on the extreme left and right (between primed and unprimed symbols), $\bar{w}$ must begin [and end]. Hence, letting w be the portion of $\bar{w}$ up to the first],

$$w = [u * \cdots *' v],$$

where to begin with we have the correspondences

$$w = [u * | \cdots *' v |],$$

$$w = [| u * \cdots | *' v].$$

Hence we must have $u *$ corresponding to some $r' *$ and $*' v$ to some $* s'$, where $u \Rightarrow_n^* r$ and $s \Rightarrow_n^* v$. Continuing this procedure, we see that $u \Rightarrow_n^* v$. This completes the construction and hence the proof of Theorem 4.2. $\square$

In the formal theory of languages one deals with alphabets $A = V \cup T$ where the elements of V (usually written as capital letters) are called *variables* and those of T are called *terminals*. If one of the elements of V (usually written S) is distinguished as the *start symbol* a semi-Thue process Π on A is called a *phrase structure grammar*, and the set of all words v , on the sub-alphabet T , such that $S \Rightarrow_n^* v$ is called the *language generated by Π* , written $L(\Pi)$.

Intuitively one can think of the variables as representing grammatical categories. For example, let $V = \{S, U, P, N, J, R, D\}$ where we may think of these letters as representing the categories: sentence, subject, predicate, noun, adjective, verb, adverb, respectively. Let T consist of the (lower case) letters of the English alphabet augmented by “#” (for “space”) and “.”. Here is a primitive English grammar G :

$$\begin{array}{ll} N \rightarrow \text{man} & N \rightarrow \text{woman} \\ S \rightarrow UP. & J \rightarrow \text{good} \\ U \rightarrow \text{the} \# N \# & J \rightarrow \text{bad} \\ U \rightarrow \text{the} \# J \# N \# & R \rightarrow \text{runs} \\ P \rightarrow R & R \rightarrow \text{walks} \\ P \rightarrow R \# D. & D \rightarrow \text{quickly} \\ & D \rightarrow \text{slowly.} \end{array}$$

The reader can easily verify that

$$S \xRightarrow[G]{*} \text{the} \# \text{bad} \# \text{man} \# \text{runs} \# \text{quickly}$$

so that this last is in the language generated by G .

4.3. DEFINITION. A grammar is called *context-free* if all of its productions are of the form $A \rightarrow g$ where A is a variable.

Thus our example G is context-free. We shall now show how to relate Post's correspondence problem to context-free grammars. Thus, let $\langle h_i, k_i \rangle$, $i = 1, 2, \dots, m$ be a Post correspondence system on an alphabet A . We shall construct a pair G_1, G_2 of context-free languages whose terminals consist of A together with m new symbols $c_1, \dots, c_m$.

In addition, the alphabet of G_1 has the single variable S_1 as start symbol and that of G_2 the single variable S_2 as its start symbol. The productions of G_1 are

$$\left. \begin{array}{l} S_1 \rightarrow h_i S_1 c_i \\ S_1 \rightarrow h_i c_i \end{array} \right\} i = 1, 2, \dots, m,$$

and those of G_2 are

$$\left. \begin{array}{l} S_2 \rightarrow k_i S_2 c_i \\ S_2 \rightarrow k_i c_i \end{array} \right\} i = 1, 2, \dots, m.$$

Thus,

$$L(G_1) = \{h_{i_1} h_{i_2} \cdots h_{i_m} c_{i_m} \cdots c_{i_2} c_{i_1}\}$$

and

$$L(G_2) = \{k_{i_1} k_{i_2} \cdots k_{i_m} c_{i_m} \cdots c_{i_2} c_{i_1}\}.$$

We have at once:

4.4. LEMMA *The given Post correspondence system has a solution if and only if $L(G_1) \cap L(G_2) \neq \emptyset$.*

We conclude from Theorem 4.2:

4.5. THEOREM. *There is no algorithm to test for a given pair of context-free grammars Π_1, Π_2 whether or not $L(\Pi_1) \cap L(\Pi_2) = \emptyset$.*

4.6. DEFINITION. A phrase structure grammar Π with start symbol S is called *ambiguous* if for some word $u \in L(\Pi)$, we have

$$S \xRightarrow{\Pi} u_1 \xRightarrow{\Pi} u_2 \xRightarrow{\Pi} \cdots \xRightarrow{\Pi} u_k = u$$

and

$$S \xRightarrow{\Pi} v_1 \xRightarrow{\Pi} v_2 \xRightarrow{\Pi} \cdots \xRightarrow{\Pi} v_l = u$$

where the sequences $\langle u_1, \dots, u_k \rangle$ and $\langle v_1, \dots, v_l \rangle$ are not the same.

Now, let G_1, G_2 be as above. Let G have the same terminals as G_1 and G_2 , the variables S, S_1, S_2 (with S as start symbol), and the productions $S \rightarrow S_1, S \rightarrow S_2$ together with the productions of G_1 and G_2 . Then, clearly, $L(G) = L(G_1) \cup L(G_2)$. Because G_1 and G_2 are themselves not ambiguous, it is easy to see that G is ambiguous just in case there is a word u which simultaneously belongs to $L(G_1)$ and to $L(G_2)$.

Using the proof of Theorem 4.5, we have:

4.7. THEOREM. *There is no algorithm by means of which we can test a given context-free grammar to determine whether or not it is ambiguous.*

For other examples of unsolvable problems in the formal theory of languages and further references, see HOPCROFT and ULLMAN [1969]. In PATERSON [1970] it is shown, using the unsolvability of Post's correspondence problem, that there is no algorithm which can be used to determine of a given finite set of 3×3 matrices with integer entries, whether or not some finite product of members of the set is equal to the zero matrix.

Another combinatorial problem which has turned out to be unsolvable is the *problem of tag*, first studied by E. L. Post in the 1920's. Cf. POST [1943, 1965]. A *tag process* is given by an alphabet $A = a_1, \dots, a_n$, n words $g_1, \dots, g_n$ and a positive integer k . For such a tag process T , we write $u \Rightarrow_T v$ if u begins with a_i and v is obtained from u by placing g_i at its right-hand end and then crossing out the first k symbols of u . (Of course, it is possible that $v = \Lambda$.) As before, we write $u \Rightarrow_T^* v$ to mean that $u = u_1 \Rightarrow_T u_2 \Rightarrow_T \cdots \Rightarrow_T u_n = v$ for words $u_1, \dots, u_n$ and some $n \geq 1$, and speak of the word problem for T as the problem of determining for given u, v whether or not $u \Rightarrow_T^* v$. MINSKY [1961, 1967] showed how to construct a tag process with an unsolvable word problem.

5. Diophantine equations

We have already mentioned Hilbert's tenth problem (cf. the Introduction), which sought an algorithm for testing polynomial equations $P(x_1, \dots, x_n) = 0$ (with integer coefficients) for possession of a solution in integers. In this section it will be more convenient to work with non-

negative integer solutions, i.e. solutions in $\mathbb{N}$. We therefore begin by noting that once it has been established that there is no algorithm for testing polynomial equations for possession of solutions in $\mathbb{N}$, it will follow at once that there can be no algorithm which can test for arbitrary integer solutions. For, if we had an algorithm which could test for integer solutions (i.e. a solution to Hilbert's tenth problem), we could use it to decide whether or not $P(x_1, \dots, x_n) = 0$ has a solution in $\mathbb{N}$ by simply testing

$$P(u_1^2 + v_1^2 + y_1^2 + z_1^2, \dots, u_n^2 + v_n^2 + y_n^2 + z_n^2) = 0$$

for having an integer solution. (This works because every non-negative integer is the sum of 4 squares.)

Our discussion will revolve about the notion of Diophantine set:

5.1. DEFINITION. A k -ary relation R on $\mathbb{N}$ is *Diophantine* if for some polynomial $P(x_1, \dots, x_k, y_1, \dots, y_n)$ with integer coefficients, we have:

$$R = \{\langle x_1, \dots, x_k \rangle : \exists y_1, \dots, y_n \in \mathbb{N} [P(x_1, \dots, x_k, y_1, \dots, y_n) = 0]\}.$$

Let R be a Diophantine relation and let $g_R: \mathbb{N}^k \rightarrow \mathbb{N}$ be defined by $g_R(x_1, \dots, x_k) = 0$ if $\langle x_1, \dots, x_k \rangle \in R$ and $g_R(x_1, \dots, x_k)$ is undefined otherwise. If R is connected to the polynomial P as in 5.1, an algorithm for computing the partial function g_R is to effectively arrange all n -tuples $\langle y_1, \dots, y_n \rangle$ in a suitable sequence and to successively evaluate $P(x_1, \dots, x_k, y_1, \dots, y_n)$ until (if ever) the value 0 is obtained. Using Church's thesis, we conclude that g_R is a recursive partial function, and hence that there is a Turing machine which computes g_R . Hence, by Definition 1.3, we conclude that R is recursively enumerable:

5.2. THEOREM. *Every Diophantine relation is r.e.*

The main theorem of the subject is the converse:

5.3. THEOREM (MATIJACEVIĆ [1970]). *Every r.e. relation is Diophantine.*

A detailed proof of Theorem 5.3 and a historical discussion can be found in the survey article DAVIS [1973] (in which, however, recursive functions are not defined in terms of Turing machines), and various of its ramifications are discussed in DAVIS, MATIJACEVIĆ and ROBINSON [1976]. We also refer the reader to these papers for further references.

Before discussing the proof of Theorem 5.3, we consider some of its consequences. Using Theorems 1.5 and 5.3 we have:

5.4. COROLLARY. *There is a Diophantine set K which is not recursive.*

Writing

$$K = \{x: \exists y_1, \dots, y_n [P(x, y_1, \dots, y_n) = 0]\}$$

we see that there can be no algorithm for testing each of the equations:

$$P(0, y_1, \dots, y_n) = 0,$$

$$P(1, y_1, \dots, y_n) = 0,$$

...

for having a solution in $\mathbb{N}$. Hence Hilbert's tenth problem is unsolvable.

For any polynomial $P(x_1, \dots, x_k)$ let us write $\#(P)$ for the cardinal number of the set of k -tuples of elements of $\mathbb{N}$ which satisfy the equation $P = 0$. Thus $0 \leq \#(P) \leq \aleph_0$. Let us call a set of cardinal numbers $\leq \aleph_0$ *non-trivial* if the set is non-empty and it does not contain all cardinal numbers $\leq \aleph_0$. Then, we shall prove:

5.5. THEOREM (DAVIS [1972]). *Given a non-trivial set A of cardinal numbers $\leq \aleph_0$, there is no algorithm which can be used to test a given polynomial P for whether or not $\#(P) \in A$.*

Thus, there is no algorithm to test whether a Diophantine equation has an even number of solutions, an infinite number of solutions, etc. The proof we give is a simplified version due to Smorynski. (Cf. also DAVIS, MATIJACEVIČ and ROBINSON [1976].)

Now, for each polynomial $P(x_1, \dots, x_k)$ we write

$$T^+(P) = P(x_1, \dots, x_k) \cdot [(x_1 - a_1)^2 + \dots + (x_k - a_k)^2],$$

where $\langle a_1, \dots, a_k \rangle$ is the first (in any convenient ordering) k -tuple which fails to satisfy $P = 0$. Thus

$$\#(T^+(P)) = \#(P) + 1.$$

Setting, $T^0(P) = P$, $T^{m+1}(P) = T^+(T^m(P))$, we have:

$$\#(T^m(P)) = \#(P) + m.$$

Finally we write

$$T^\infty(P) = (u + 1) \cdot P$$

where u is a variable which does not occur in P . Here

$$\#(T^\infty(P)) = \begin{cases} 0 & \text{if } \#(P) = 0, \\ \aleph_0 & \text{if } \#(P) \neq 0. \end{cases}$$

The proof of 5.5 proceeds by cases:

Case 1. $A = \{0\}$. This is just the question of testing a Diophantine equation for possession of a solution which we have seen to be unsolvable.

Case 2. $0, \aleph_0 \in A$. Let $m \notin A$. Then,

$$\#(P) = 0 \leftrightarrow \#(T^m(T^\infty(P))) \notin A.$$

Hence an algorithm for this case would yield one for case 1.

Case 3. $0 \in A, \aleph_0 \notin A$. Then,

$$\#(P) = 0 \leftrightarrow \#(T^\infty(P)) \in A$$

and once again we have a reduction to case 1.

Case 4. $0 \notin A$. Then the set B of cardinal numbers $\leq \aleph_0$ not in A is in case 2 or case 3. But an algorithm for testing $\#(P) \in A$ is equivalent to one for testing $\#(P) \in B$.

Using the normal form theorem (ERT 4.1), i.e. the existence of a universal Turing machine, we infer the existence of a Diophantine equation $P(i, x, y_1, \dots, y_k) = 0$ which is universal in the sense that, setting

$$D_i = \{x: \exists y_1, \dots, y_k [P(i, x, y_1, \dots, y_k) = 0]\}$$

the sequence $D_0, D_1, D_2, \dots$ is a list of *all* Diophantine subsets of $\mathbb{N}$. There has been considerable interest in finding the best value of k in this result. In MATIJACEVIĆ and ROBINSON [1975], it is shown that we can take $k = 13$; more recently Matijacević has announced that this result can be improved to $k = 9$.

This is an appropriate place to discuss an unsolvable decision problem that was obtained quite early in the history of the subject (CHURCH [1936]; TURING [1936]), the unsolvability of the problem determining of for a finite set of sentences T and a sentence ϕ of first order logic, whether or not $T \vdash \phi$ in first order logic, cf. the introductory Chapter A.1. Now, Hilbert had declared that this very problem, the so-called Entscheidungsproblem, was the fundamental problem of mathematical logic, because a procedure for solving it could presumably be used to algorithmically settle all mathematical questions. (See the discussion of Hilbert's thesis in Section 5 of Chapter A.1.) Hence once one knows that there are unsolvable mathematical problems, one should expect to be able to readily infer the unsolvability of the Entscheidungsproblem. We shall see how this can be done easily using the unsolvability of Hilbert's tenth problem.

Let us consider the language

$$L = \{+, \cdot, 0, 1\}$$

where 0, 1 are constant symbols and $+$, $\cdot$ are 2-ary function symbols. Here the structure $\mathbb{N} = \langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ is a structure for L . Now, given a Diophantine equation $P = 0$, it is easy to construct a sentence ϕ of L of the form $\exists y_1 \cdots \exists y_k (t_1 = t_2)$ where t_1 and t_2 are terms, such that $\mathbb{N} \models \phi$ if and only if the equation $P = 0$ is solvable. Let T be the set of sentences

$$((0 + 1) = 1)$$

$$\forall x ((x + 0) = x)$$

$$\forall x \forall y ((x + (y + 1)) = (x + y) + 1))$$

$$\forall x ((x \cdot 0) = 0)$$

$$\forall x \forall y ((x \cdot (y + 1)) = ((x \cdot y) + x)).$$

Then it is clear that for any equation θ between terms of L containing no variables, $\mathbb{N} \models \theta$ if and only if $T \vdash \theta$, because T obviously suffices to justify specific calculations in $\mathbb{N}$. Finally using the appropriate rule of first order logic for introducing existential quantifiers we have:

$$T \vdash \phi \quad \text{if and only if} \quad P = 0 \text{ has a solution.}$$

From the unsolvability of Hilbert's tenth problem, we then immediately conclude that the Entscheidungsproblem for L is unsolvable. For sharper results see KAHN, MOORE and WANG [1962] and AANDERAA and LEWIS [1974].

We now discuss the proof of Theorem 5.3. Clearly, since

$$P_1 = 0 \wedge P_2 = 0 \leftrightarrow P_1^2 + P_2^2 = 0,$$

$$P_1 = 0 \vee P_2 = 0 \leftrightarrow P_1 \cdot P_2 = 0,$$

the class of Diophantine relations is closed under union and intersection. Hence Diophantine "definitions" can be combined using $\wedge$, $\vee$ and existential quantifiers to yield new definitions of Diophantine relations. Also the relations $x < y$, $x \leq y$, $x \equiv y \pmod{z}$ are clearly Diophantine since

$$x < y \leftrightarrow \exists z (x + z + 1 = y)$$

$$x \leq y \leftrightarrow \exists z (x + z = y)$$

$$x \equiv y \pmod{z} \leftrightarrow \exists t (x + tz = y \vee y + tz = x).$$

The steps in the proof of Theorem 5.3 are as follows:

(i) *The relation $z = x^y$ is Diophantine.* This key step came last historically. We shall not give a proof here but refer the reader to *any* of the following for a detailed proof: MATIJACEVIĆ [1972], DAVIS [1971, 1973], MATIJACEVIC and ROBINSON [1975].

(ii) *The relations $m = \binom{n}{k}$, $m = n!$ are Diophantine.* Let us write $\Phi(k, u, w)$ for the coefficient of u^k in the u -ary expansion of w . Then the relation

$$q = \Phi(k, u, w)$$

is a Diophantine relation. For, the relation can be expressed as the simultaneous solvability in $\mathbb{N}$ of the conditions:

$$\begin{aligned} w &= p + qu^k + r, \\ q &< u, \quad p < u^k, \\ r &\equiv 0 \pmod{u^{k+1}}. \end{aligned}$$

Now if $u > 2^n$, the expansion

$$(u+1)^n = \sum_{i=0}^n \binom{n}{i} u^i$$

shows that $\binom{n}{k}$ is just the coefficient of u^k in the u -ary expansion of $(u+1)^n$. Hence

$$m = \binom{n}{k} \leftrightarrow m = \Phi(k, 2^n + 1, (u+1)^n)$$

so that $m = \binom{n}{k}$ is Diophantine.

Elementary inequalities show that when $r > (2n)^{n+1}$ we have

$$n! < \frac{r^n}{\binom{r}{n}} < n! + 1.$$

(For details see for example DAVIS [1973]) Hence,

$$\begin{aligned} m = n! \leftrightarrow \exists r \exists s \exists t \exists u \left\{ s = 2n + 1 \ \& \ r = s' \ \& \ t = r^n \ \& \ u = \binom{r}{n} \right. \\ \left. \& \ um < t < u(m+1) \right\} \end{aligned}$$

(iii) *The bounded quantifier theorem.* Let $P(u, x, y, h, z_1, \dots, z_n)$ be a polynomial. Then, there is a polynomial $Q(u, x, y)$ such that

$$\forall k \leq x \exists z_1, \dots, z_n \leq y [P(u, x, y, k, z_1, \dots, z_n) = 0] \leftrightarrow$$

$$\leftrightarrow \exists b_1, \dots, b_n \left[\binom{b_1}{y+1} \equiv \dots \equiv \binom{b_n}{y+1} \equiv \right.$$

$$\left. P(u, x, y, Q! - 1, b_1, \dots, b_n) \equiv 0 \pmod{\binom{Q! - 1}{x+1}} \right].$$

This is an improved version of a result from DAVIS, PUTNAM and ROBINSON [1961]. For its proof see DAVIS, MATIJACEVIĆ and ROBINSON [1976], p. 21.

(iv) We now have:

5.6. THEOREM. *Let R be a Diophantine relation and let*

$$\langle x_1, \dots, x_k, x \rangle \in S \leftrightarrow \forall t \leq x [\langle x_1, \dots, x_k, t \rangle \in R].$$

Then S is Diophantine.

PROOF. We have for a suitable polynomial P ,

$$\langle x_1, \dots, x_k, x \rangle \in S \leftrightarrow \forall t \leq x \exists z_1, \dots, z_n [P(t, x_1, \dots, x_k, z_1, \dots, z_n) = 0]$$

$$\leftrightarrow \exists y \forall t \leq x$$

$$\exists z_1, \dots, z_n \leq y [P(t, x_1, \dots, x_k, z_1, \dots, z_n) = 0]$$

since the bound y can be chosen as the largest of $n(x+1)$ integers. The result follows from (ii) and (iii). $\square$

(v) Now let P be an arbitrary k -ary r.e. relation. Let T be a Turing machine with instructions $q_0, \dots, q_\nu$ such that T eventually halts when started at q_0 scanning the leftmost symbol of $\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$ if and only if $\langle x_1, x_2, \dots, x_k \rangle \in P$. Let T' be obtained from T by adjoining to its table all quintuples:

$$i \alpha \quad \alpha R (\nu + 1)$$

where $0 \leq i \leq \nu$ and the table of T has no quintuple beginning $i \alpha$. Thus $\langle x_1, \dots, x_k \rangle \in P$ if and only if T' eventually encounters instruction $q_{\nu+1}$ (and then halts) when started at q_0 scanning the leftmost symbol of $\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$.

We shall code configurations of T' by triples $\langle l, n, r \rangle$ of natural numbers. Here n is simply the number of the instruction about to be executed and l is a code for the sequence of 0's and 1's on the tape to the left of the scanned square; specifically l is just the natural number whose binary representation is this sequence (where of course the infinite sequence of 0's

on the left has no effect on l). Similarly r is the natural number whose binary representation is the sequence of 0's and 1's beginning with and to the right of the scanned square, *read from right to left*. Thus, for example, the tuple $\langle 13, 4, 19 \rangle$ represents a machine configuration in which the tape contents are

$$\dots 000110111001000\dots,$$

the scanned square contains 1 as do its left and right immediate neighbors, and instruction q_4 is about to be executed.

The initial configuration of T' with inputs $x_1, \dots, x_k$ is represented by the triple $\langle 0, 0, g_k(x_1, \dots, x_k) \rangle$, where

$$g_1(x) = 2^{x+1} - 1$$

$$g_{k+1}(x_1, \dots, x_{k+1}) = 2g_k(x_2, \dots, x_{k+1}) + g_1(x_1).$$

Here, as we verify by an easy induction, the relation $z = g_k(x_1, \dots, x_k)$ is Diophantine for each *fixed* k .

For Q a quintuple from the table of T' , let S_Q be the set of all $\langle l, n, r, l', n', r' \rangle$ such that Q acts on configuration $\langle l, n, r \rangle$ to produce configuration $\langle l', n', r' \rangle$. For each fixed quintuple Q , S_Q is a Diophantine relation as we proceed to show.

For, if Q has the form

$$i \alpha \quad \beta R j,$$

then

$$\langle l, n, r, l', n', r' \rangle \in S_Q \Leftrightarrow n = i \wedge n' = j \wedge l' = 2l + \beta \wedge r' = 2r + \alpha.$$

On the other hand, if Q has the form

$$i \alpha \quad \beta L j,$$

then

$$\begin{aligned} \langle l, n, r, l', n', r' \rangle \in S_Q &\Leftrightarrow \\ &\Leftrightarrow n = i \wedge n = j \wedge [(l = 2l' \wedge r' = 2(r + \beta - \alpha)) \vee \\ &\quad (l = 2l' + 1 \wedge r' = 2(r + \beta - \alpha) + 1)]. \end{aligned}$$

Let $Q_1, Q_2, \dots, Q_\mu$ be a list of *all* of the quintuples from the machine table of T' and let $S = \bigcup_{i=1}^\mu S_{Q_i}$. Thus, S is a Diophantine relation and $\langle l, n, r, l', n', r' \rangle \in S$ just in case some quintuple of T' acts on configuration $\langle l, n, r \rangle$ to produce configuration $\langle l', n', r' \rangle$.

Now a computation of T' is a sequence of configurations $\langle l_i, n_i, r_i \rangle$, $i = 0, 1, \dots, k+1$ such that $\langle l_i, n_i, r_i, l_{i+1}, n_{i+1}, r_{i+1} \rangle \in S$ for $i = 0, 1, \dots, k$ and $n_{k+1} = \nu + 1$. We shall regard the numbers l_i, n_i, r_i as *digits* to a sufficiently large base B , i.e. we set

$$L = \sum_{i=0}^k l_i B^i, \quad N = \sum_{i=0}^k n_i B^i, \quad R = \sum_{i=0}^k r_i B^i.$$

Using the function Φ from (ii), we have finally,

$$\langle x_1, \dots, x_k \rangle \in P \Leftrightarrow$$

$$\Leftrightarrow \exists B, L, N, R, k \{ \Phi(0, B, L) = 0 \wedge \Phi(0, B, N) = 0 \wedge$$

$$\Phi(0, B, R) = g_k(x_1, \dots, x_k) \wedge \Phi(k+1, B, N) = \nu + 1 \wedge$$

$$\forall i \leq k [\langle \Phi(i, B, L), \Phi(i, B, N), \Phi(i, B, R),$$

$$\Phi(i+1, B, L), \Phi(i+1, B, N),$$

$$\Phi(i+1, B, R) \rangle \in S] \}.$$

Using Theorem 5.6, it follows that P is Diophantine.

References

AANDERAA, S.

[1973] A proof of Higman's embedding theorem using Britton extensions of groups, in: BOONE, CANNONITO and LYNDON [1973], pp. 1-18.

AANDERAA, S. and H.R. LEWIS

[1974] Linear sampling and the $\forall\exists\forall$ case of the decision problem. *J. Symbolic Logic*, **39**, 519-548.

ADJAN, S.I.

[1955] The algorithmic unsolvability of problems concerning certain properties of groups (in Russian), *Dokl. Akad. Nauk SSSR*, **103**, 533-535.

BOONE, W.W.

[1959] The word problem, *Ann. of Math.*, **70**, 207-265.

BOONE, W.W., F.B. CANNONITO and R.C. LYNDON

[1973] *Word Problems* (North-Holland, Amsterdam).

BOONE, W.W., W. HAKEN and V. POENARU

[1968] On recursively unsolvable problems in topology and their classification, in: *Contributions to Mathematical Logic*, edited by H.A. Schmidt et al. (North-Holland, Amsterdam) pp. 37-74.

BRITTON, J.L.

[1963] The word problem, *Ann. of Math.*, **77**, 16-32.

CHURCH, A.

[1936] A note on the Entscheidungsproblem, *J. Symbolic Logic*, **1**, 40-41, 101-102. [Corrected version in: DAVIS [1965], pp. 108-115.]

DAVIS, M

[1965] *The Undecidable* (Raven Press, Hewlett, NY).

[1971] An explicit Diophantine definition of the exponential function, *Comm. Pure Appl. Math.*, **24**, 137-145.

[1972] On the number of solutions of Diophantine equations. *Proc. Am. Math. Soc.*, **35**, 552-554.

[1973] Hilbert's Tenth Problem is unsolvable, *Am. Math. Monthly*, **80**, 233-269.

DAVIS, M., YU. MATIJACEVIČ and J. ROBINSON

- [1976] Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution, *Proc. Symposia Pure Math.*, **28**, 223–378.

DAVIS, M., H. PUTNAM and J. ROBINSON

- [1961] The decision problem for exponential Diophantine equations, *Ann. of Math.*, **74**, 425–436.

HAKEN, W.

- [1973] Connections between topological and group theoretical decision problems, in: BOONE, CANNONITO and LYNDON [1973], pp. 427–441.

HIGMAN, G.

- [1961] Subgroups of finitely presented groups, *Proc. Roy. Soc. London Ser. A*, **262**, 455–475.

HOPCROFT, J. and J. ULLMAN

- [1969] *Formal Languages and their Relation to Automata* (Addison-Wesley, Reading, MA).

KAHR, A.S., E.F. MOORE and H. WANG

- [1962] Entscheidungsproblem reduced to the AEA case, *Proc. Nat. Acad. Sci. U.S.A.*, **48**, 365–377.

MARKOV, A.A.

- [1947] On the impossibility of certain algorithms in the theory of associative systems (in Russian), *Dokl. Akad. Nauk SSSR*, **55**, 587–590. [English translation in *C.R. Acad. Sci. URSS*, **55**, 533–586.]
- [1958] Unsolvability of the problem of homeomorphy (in Russian), in: *Proceedings of the International Congress of Mathematicians* (Cambridge University Press, London), pp. 300–306.

MATIJACEVIČ, YU.

- [1970] Enumerable sets are Diophantine. *Dokl. Akad. Nauk SSSR*, **191**, 279–282. [Improved English translation in *Soviet Math. Doklady*, **11**, 354–357.]
- [1972] Diophantine sets, *Uspehi Mat. Nauk*, **27**, 185–222. [English translation in *Russian Math. Surveys*, **27**, 124–164.]

MATIJACEVIČ, YU. and J. ROBINSON

- [1975] Reduction of an arbitrary Diophantine equation to one in 13 unknowns, *Acta Arith.*, **27**, 521–553.

McKENZIE, R. and R.J. THOMPSON

- [1973] An elementary construction of unsolvable word problems in group theory, in: BOONE, CANNONITO and LYNDON [1973], pp. 457–478.

MINSKY, M.

- [1961] Recursive unsolvability of Post's problem of tag and other topics in the theory of Turing machines, *Annals of Math.*, **74**, 437–454.
- [1967] *Computation: Finite and Infinite Machines* (Prentice-Hall, Englewood Cliffs, NJ).

NOVIKOFF, P.S.

- [1955] On the algorithmic unsolvability of the word problem in group theory (in Russian), *Dokl. Akad. Nauk SSSR Matematicheskii Institut Trudy*, **44**, Moscow.

PATERSON, M.S.

- [1970] Unsolvability in 3×3 matrices, *Studies in Appl. Math.*, **49**, 105–107.

POST, E.L.

- [1943] Formal reductions of the general combinatorial decision problem, *Am. J. Math.*, **65**, 197–215.
- [1946] A variant of a recursively unsolvable problem, *Bull. Am. Math. Soc.*, **52**, 264–268.
- [1947] Recursive unsolvability of a problem of Thue. *J. Symbolic Logic*, **12**, 1–11. [Reprinted in: DAVIS [1965], pp. 293–303.]

- [1965] Absolutely unsolvable problems and relatively undecidable propositions. Account of an anticipation, in: DAVIS [1965], pp. 340–433.
- RABIN, M.O.
[1958] Recursive unsolvability of group theoretic problems, *Ann. of Math.*, **67**, 172–194.
- ROTMAN, J.J.
[1973] *The Theory of Groups* (Allyn and Bacon, Boston, MA, 2nd edition).
- SHOENFIELD, J.R.
[1967] *Mathematical Logic* (Addison-Wesley, Reading, MA).
- THUE, A.
[1914] Probleme über Veränderungen von Zeichenreihen nach gegebenen Regeln, *Skr. utgitt av Vid. Kristiania, I. Mat.-Naturv. Klasse*, **10**.
- TURING, A.M.
[1936] On computable numbers, with an application to the Entscheidungsproblem, *Proc. London Math. Soc.*, Ser. 2, **42**, 230–265; **43**, 544–546. [Reprinted in: DAVIS [1965], pp. 116–154.]
- YASUHARA, A.
[1971] *Recursive Function Theory and Logic* (Academic Press, New York).

Decidable Theories

MICHAEL O. RABIN

Contents

Survey and basic notions	596
1. The method of elimination of quantifiers	600
1.1 Theories and models	600
1.2 Elimination of quantifiers for discrete orders	603
1.3 Presburger's arithmetic	606
1.4 Theory of real numbers	606
1.5 Other theories	607
2. Model theoretic methods	607
2.1 Categoricity, completeness and decidability	607
2.2 Algebraically closed fields	608
2.3 Real-closed fields	609
2.4 Theory of DO revisited	610
2.5 Further results	611
3. The method of interpretations	612
3.1 Semantic interpretations	612
3.2 Decidable second-order theories	615
3.3 The tree theorem	616
3.4 Presburger's arithmetic revisited	617
3.5 Second-order theory of linear order	617
3.6 Decidability in topology	618
3.7 Boolean algebras	619
3.8 Non-classical logics	620
4. Complexity of decision procedures	621
4.1 Turing-machine computations	621
4.2 The theory WS1S	623
4.3 Theories of addition and real-closed fields	624
4.4 Propositional calculus and $P = NP$	625
References	627

Survey and basic notions

The study of *decidability* involves trying to establish, for a given mathematical *theory* T , or a given problem P , the existence of a decision algorithm AL which will accomplish the following task. Given a sentence A expressed in the language of T , the algorithm AL will determine whether A is true in T , i.e. whether $A \in T$. In the case of a problem P , given an instance I of the problem P , the algorithm AL will produce the correct answer for this instance. Depending on the problem P , the answer may be “yes” or “no”, an integer, etc.

If such an algorithm does exist, then we shall variously say that the *decision problem* of T or P is *solvable*, or that the theory T is *decidable*, or simply that the problem P is solvable. Of AL we shall say that it is a *decision procedure* for T or P . Let us illustrate our concepts by two celebrated decidability results.

Let L be a first-order language appropriate for expressing statements about planar Euclidean Geometry. Thus L has individual variables ranging over points; two ternary predicates $L(x, y, z)$ and $B(x, y, z)$ to denote collinearity and betweenness; two predicates $C(x, y, z, u, v, w)$ and $A(x, y, z, u, v, w)$ to denote congruence of triangles and congruence of angles (i.e. $\Delta xyz \cong \Delta uvw$ and $\sphericalangle xyz = \sphericalangle uvw$); and a quaternary predicate $E(x, y, u, v)$ to denote equality of length (i.e. $\overline{xy} = \overline{uv}$). The formula

$$\forall xyzuv [A(x, y, v, z, y, v) \wedge A(x, z, u, y, z, u) \wedge B(x, y, u) \wedge B(x, z, v) \wedge E(u, z, v, y) \rightarrow E(x, y, x, z)],$$

for example, is an expression in L of the famous high school problem to the effect that if in a triangle the angle bisectors are equal, then the triangle is isosceles.

TARSKI [1951] has proved that the theory EG consisting of all sentences of L true in planar Euclidean Geometry, the so-called elementary geometry, is decidable.

Actually Tarski proved a stronger result. Let $\mathfrak{R} = \langle R, +, \cdot \rangle$ be the field of real numbers, then the first-order theory $\text{Th}(\mathfrak{R})$ is decidable. This last result implies the decidability of elementary geometry via the introduction of Cartesian coordinates and the reduction of geometric statements to equivalent algebraic statements.

Our second example is also related to Euclid. The problem GCD consists of finding for pairs a, b of natural numbers their greatest common divisor (a, b) . A slight variant of the famous Euclid's algorithm is based on

the facts that $(a, 0) = a$ and, for $a \leq b$, $(a, b) = (a, b - a)$. A succession of steps of the second type will transform any g.c.d. (a, b) into $(c, 0)$, so that $(a, b) = c$. Thus $(27, 15) = (12, 15) = (12, 3) = (9, 3) = (6, 3) = (3, 3) = (3, 0) = 3$.

The assignment of a precise mathematical meaning to decidability involves the notion of a computable or recursive function. By an appropriate Gödel numbering G , the set of all sentences of a language L is 1-1 mapped onto a recursive subset $S \subseteq \mathbb{N}$ of the set $\mathbb{N}$ of natural numbers. This transforms T into a set $G(T) \subseteq S$. The theory T is, by definition, decidable if and only if $G(T)$ is a recursive set, i.e. its characteristic function f_T is computable. Solving the decision problem of T involves producing a program or algorithm for computing f_T , or at least proving that f_T is computable. The notion of solvability of a problem P is explicated in a similar fashion.

As explained elsewhere in this volume, the theory T is defined to be *undecidable* if f_T is not recursive.

There is a significant methodological difference between the study of decidability and the study of undecidability, and this despite the obvious fact that the two concepts are just the opposite sides of the same coin. Attempts to establish the undecidability of a theory T must presuppose a mathematically precise notion of computable functions. For only after we know what a computable function is, can we prove that f_T is not computable.

On the other hand, the decision problem of a theory T can be solved by exhibiting a decision algorithm AL which is directly recognized and accepted by mathematicians as being an effective computational procedure. Thus, for example, Euclid's algorithm given above, when supplemented by explicit rules for comparison and subtraction of natural numbers, is universally agreed upon as constituting a computational method.

This state of affairs accounts for the historical fact that some decidability results preceded the definition of recursive functions in the mid-Thirties, whereas the first undecidability results only followed the formulation of this definition.

There are three main methods for establishing decidability of theories. The first and oldest is elimination of quantifiers. This method consists of transforming the given sentence A into another sentence B such that $T \vdash A \leftrightarrow B$ and B belongs to a class $\mathcal{K}$ of sentence for the members of which we can directly determine whether they are in T .

The second method is model-theoretic. In its typical form it involves a

(recursive) set of axioms AX for the theory T . Model-theoretic methods are employed to either show that AX is complete, in which case T is readily seen to be decidable, or to systematically survey all completions of AX . In the latter case we shall know for each sentence A whether $T \cup \{\neg A\}$ is consistent and consequently whether $T \vdash A$.

In certain cases a combination of the two methods is used. Namely a set $\mathcal{K}$ of sentences of L is judiciously chosen, the fact that for every sentence A of L there exists a sentence $B \in \mathcal{K}$ equivalent to A by T is then established by model-theoretic means. Also the sentences $B \in \mathcal{K}$ true in T are picked out by a survey of models of T .

The third method involves interpretations. Let T_0 be a theory known to be decidable, and let T be any theory. Assume that we have a (computable) map t which transforms or translates each sentence A of the language L into a sentence $t(A)$ of the language L_0 so that $t(A) \in T_0$ if and only if $A \in T$. Under these conditions T is decidable. For in order to determine whether $A \in T$ we just find $t(A)$ and check whether $t(A) \in T_0$. Usually the interpretation t involves model-theoretic considerations. It is shown that models of T can be isomorphically reproduced from models of T_0 by relations definable in L_0 . This method was used in RABIN [1969] to establish most of the then known decidability results as well as several new ones.

The method of interpretations is, *mutatis-mutandis*, also a powerful tool for proofs of undecidability. For if the theory T is known to be undecidable, and is interpretable in T_0 in the manner of the previous paragraph, then T_0 must be undecidable, see RABIN [1965].

The study of decidability should be viewed as a component, or natural outgrowth, of Hilbert's Program for the foundations of mathematics. Hilbert envisioned a codification of the various branches of mathematics by systems of axioms, with an axiomatized logic serving as a common basis for deduction of consequences (theorems) from the axioms. Hilbert hoped that such a formalization would turn the derivation of mathematical results into a mechanical game with strings of symbols. According to Hilbert's plan, this would give us such a comprehensive survey of all formal theorems within any mathematical discipline, that we would be able to demonstrate that no formal statement and its negation are jointly provable, thereby demonstrating the consistency of mathematics. Also implied by Hilbert's Programme is the belief that the process of theorem-proving is mechanizable or, in modern parlance, that mathematical theories are decidable. Failing to implement Hilbert's plan for mathematics as a whole, by proving the consistency and decidability of, say, set theory, researchers turned their

attention to more restricted segments of mathematics. Many of the decidability results which we shall discuss later on, such as Presburger's decision method for the theory of addition of natural numbers, were obtained in the Twenties and early Thirties and were motivated by Hilbert's plan.

Gödel's celebrated Incompleteness Theorems and Church's Undecidability result, dating back to the early and mid-Thirties, dashed the hopes for realization of Hilbert's Programme in its original form. Namely, Gödel demonstrated the impossibility of proving the consistency of any appreciable portion of mathematics by the finitist methods advocated by Hilbert. And Church proved that the predicate calculus, as well as the arithmetic of addition and multiplication of natural numbers, are undecidable. These results put into perspective the study of decidability and engendered a considerable body of research into the decidability and undecidability of various mathematical theories.

Only in recent years attention turned to the issue of the computational complexity of solvable decision problems. In the spirit of Hilbert's Programme and of Turing's analysis of computability, it was tacitly assumed that for a theory T proved decidable, the question whether a given sentence is a theorem of T is a trivial one. For one needs only to mechanically apply the decision procedure in order to answer any such question. No creative or intelligent thinking is required for this process. From this point of view, any decidable theory is trivial and uninteresting. Work of Fischer, Meyer, Rabin, and others has caused a reevaluation of this attitude. They have shown that many theories, even though decidable, are from the practical point of view undecidable because any decision algorithm would require a practically impossible number of computation steps. For the arithmetic of addition of natural numbers, proved decidable by Presburger, FISCHER and RABIN [1974] have proved that for every decision algorithm AL there exist sentences A of size (i.e. number of symbols) n such that AL requires 2^{2^n} computational steps to decide A . MEYER [1975] has proved even more devastating complexity results for theories such as the theory of linear-order. Fischer and Rabin have also shown that Elementary Geometry has a decision problem which is inherently of exponential complexity. Results such as these cast doubt on the assertion that any theory proved decidable is trivial because its theorems could be checked by a computer program. Computations involving, say, $2^{2^{30}}$ steps cannot be considered as a feasible method for establishing the truth of a mathematical statement.

Are there any theories with a practically solvable decision problem?

Startlingly enough the answer to this fundamental question is as yet unknown. It is readily seen that the decision problem of any formalized theory is at least as complex as the decision problem PC of the propositional calculus. Now Cook [1971] has observed that many combinatorial decision problems which have defied attempts at producing an efficient, not exponentially complex, decision procedure, are reducible to PC. This lends credence to the conjecture that PC is exponentially complex. Cook has related this question, via a use of Turing machines, to the question whether non-deterministic computations requiring a number of steps polynomial in the problem size, are always equivalent to ordinary deterministic computations requiring a polynomial number of steps. This so-called $P = NP$ problem is, as of the time of writing of this paper, one of the central open questions in theoretical computer science. It also relates to the older "spectrum problem" concerning models of sentences of the predicate calculus. Details will be given in the text.

Since the study of decidability involves methods from propositional and predicate logic, theory of computable functions, and theory of models, we shall have to rely on these prerequisites in our exposition. In most cases only the rudiments of these subjects will be required for following discussions. The uninitiated reader is urged to consult the relevant chapters of this book for any auxiliary information that he may need.

1. The method of elimination of quantifiers

1.1. Theories and models

The theories dealt with in the study of decidability will present themselves in one of two ways: *axiomatically* or *semantically*, as the set of sentences true in a structure or class of structures. Usually we shall consider first-order theories, i.e. theories expressible in some first-order predicate language. This rule will, however, have some very important exceptions.

DEFINITION 1. Let L be some fixed first-order language and let H be a recursive consistent set of sentences of L . The *theory axiomatized by H* is, by definition, the set $\text{Th}(H)$ of all logical consequences of H

$$\text{Th}(H) = \{A \mid H \vdash A\}.$$

The theory $\text{Th}(H)$ and the set of axioms H are called *complete* if for every sentence A of L we have $A \in \text{Th}(H)$ or $\neg A \in \text{Th}(H)$.

THEOREM 1. *If the theory T is axiomatizable and complete then T is decidable.*

PROOF. Let H be an axiomatization of T . The sequences $S_i = (A_{i1}, A_{i2}, \dots, A_{in_i})$, which are formal proofs from the axioms H , can be effectively enumerated. This can be done, for example, by enumerating *all* finite sequences (words) on the alphabet of L and deleting those sequences which are not proofs. The last members A_{in_i} of the proofs enumerated run through all statements A which are provable from H , i.e. through all elements of $\text{Th}(H) = T$.

Thus, the theorems of T can be effectively (computationally) enumerated in a sequence $S = (A_1, A_2, \dots)$. Let now A be any sentence of L . Start enumerating S and for each A_n obtained check whether $A_n = A$ or whether $A_n = \neg A$. Since T is complete, one of the two alternatives must eventually occur, at which time we shall know whether $A \in T$ or $A \notin T$. $\square$

People seeing the above argument for the first time often encounter some difficulty in convincing themselves that the proposed procedure is a valid computational process for deciding T . This is because an essential feature of a computation is that we are sure it will terminate, while here when given A we have no a-priori bound on the number of steps required before the computation terminates. However, the fact that T is complete ensures that the computation will terminate by either A or $\neg A$ being encountered in the enumeration. This constitutes a proof of termination of the algorithm. In fact, the number-of-steps function is thereby shown to be a calculable function, albeit not of the commonly encountered variety such as n^n .

The idea underlying Theorem 1 can be extended to cases where the theory T is not complete.

THEOREM 2. *Let T be axiomatizable and assume that there exists a recursive (computable) sequence $A_1, A_2, \dots$, of sentences satisfying the following conditions.*

(1) $T \cup \{A_n\}$ is consistent for every n .

(2) Every completion $T \subseteq T_1$ of T has a (not necessarily recursive) set of axioms $B = \{B_1, \dots, B_k, \dots\}$ such that $T_1 = \text{Th}(B)$, and for every k there

exists an n for which $T \vdash A_n \leftrightarrow B_1 \wedge \cdots \wedge B_k$. Conditions (1)–(2) imply that T is decidable.

PROOF. Let H be a recursive axiomatization for T . By a process resembling dovetailing we can computationally enumerate in one sequence $D_1, D_2, \dots$, the logical consequences of all the sets $H_n = H \cup \{A_n\}$, $n = 1, 2, \dots$. Namely, start with an effective enumeration of the consequences of H_1 as in the proof of Theorem 1. When the first consequence $H_1 \vdash D_1$ is encountered, start enumerating consequences of H_2 until the first one, D_2 , is obtained. Now return to generate the second consequence, call it D_3 , of H_1 . Then return to H_2 to obtain $H_2 \vdash D_4$, and next obtain the first consequence, call it D_5 , of H_3 ; and so on.

Again dovetailing, effectively enumerate the above sequence $D_1, \dots, D_n, \dots$, and also the sequence $E_1, \dots, E_n, \dots$, of all consequences of H . The second sequence is, in fact, an enumeration of $T = \text{Th}(H)$. Thus, if $A \in T$ then A will appear among the E_i 's. We claim that if $A \notin T$, then $\neg A$ will appear among the D_i 's. Thus the double enumeration will computationally yield an answer to the question whether $A \in T$.

To establish the claim, note that if $A \notin T$, then $T \cup \{\neg A\}$ is consistent. Hence it is a subset of a complete theory $T \cup \{\neg A\} \subseteq T_1$. Let $B = \{B_1, B_2, \dots\}$ be the set of axioms for T_1 mentioned in the assumptions on the sequence $A_1, A_2, \dots$. Then $B \vdash \neg A$ and consequently for some integer k , $B_1 \wedge \cdots \wedge B_k \vdash \neg A$. By our assumptions there exists an n so that $T \vdash A_n \leftrightarrow B_1 \wedge \cdots \wedge B_k$. Hence $T \cup \{A_n\} \vdash \neg A$, and $\neg A$ appears in the sequence $D_1, D_2, \dots$. $\square$

Theorem 2 is used to establish decidability in cases where T is not complete and yet we can somehow survey all possible completions of T .

DEFINITION 2. Let $\mathfrak{A} = \langle A, R_1, R_2, \dots \rangle$ be a structure and L a first-order language appropriate for $\mathfrak{A}$; that is, L has a symbol P_i corresponding to any relation or function R_i of $\mathfrak{A}$. The *theory* $\text{Th}(\mathfrak{A})$ of $\mathfrak{A}$ is the set of sentences of L true in $\mathfrak{A}$

$$\text{Th}(\mathfrak{A}) = \{B \mid \mathfrak{A} \models B\}.$$

If $\mathcal{K}$ is a class of structures all of the same type, and L is a language appropriate to one and hence all structures in $\mathcal{K}$ then by definition,

$$\text{Th}(\mathcal{K}) = \bigcap_{\mathfrak{A} \in \mathcal{K}} \text{Th}(\mathfrak{A}).$$

We shall now give examples of theories defined by axioms as well as examples of theories defined by models, i.e. defined *semantically*.

EXAMPLE 1. Let L be a language with just one binary predicate symbol $\leq$ (greater or equal than). Consider the set of axioms OR:

1. $\forall x \forall y [x \leq y \wedge y \leq x \rightarrow x = y],$
2. $\forall x \forall y [x \leq y \vee y \leq x],$
3. $\forall x \forall y \forall z [x \leq y \wedge y \leq z \rightarrow x \leq z].$

Any model $\langle A, \leq \rangle \models \text{OR}$ is a totally ordered set.

Let us introduce the abbreviation $x < y$ to stand for $x \leq y \wedge \neg x = y$.

EXAMPLE 2. Consider the axioms DO obtained by adding to OR the axioms

4. $\exists x \forall y [y \leq x \rightarrow x = y],$
5. $\forall x \exists y [x < y \wedge \forall z [x < z \rightarrow y \leq z]],$
6. $\forall x \forall y [y < x \rightarrow \exists z \forall w [z < x \wedge [z < w \rightarrow x \leq w]]].$

Any model $\langle A, \leq \rangle \models \text{DO}$ is a totally ordered set which has a first element, every element has a unique immediate successor, and every element except the first element has a unique predecessor. Such orders will be called *discrete orders*.

Denoting, as usual, $\omega = \{0, 1, 2, \dots\}$ we see that $\mathfrak{N} = \langle \omega, \leq \rangle \models \text{DO}$. If we denote by ω^* the reverse order-type of ω (i.e. $0 > 1 > 2 > \dots$), then every ordered set which is a model of DO has order type $\omega + (\omega^* + \omega)\lambda$, where λ is any order type.

EXAMPLE 3. Consider the class $\mathcal{K}_{\text{uf}}$ of all structures $\langle A, f \rangle$ where f is a unary function $f: A \rightarrow A$. $\text{Th}(\mathcal{K}_{\text{uf}})$ is the theory of a unary function.

EXAMPLE 4. Let $\langle \omega, + \rangle$ be the structure of the integers with addition. $\text{Th}(\langle \omega, + \rangle) = \text{PAR}$ will be called Presburger's arithmetic or the theory of addition of natural numbers.

1.2. Elimination of quantifiers for discrete orders

Thus far we have seen examples of axiomatically defined theories and of semantically defined theories. We also gave two principles for establishing the decidability of axiomatized theories. We shall now illustrate the

method of elimination of quantifiers by proving the decidability of $\text{Th}(\langle \omega, \leq \rangle)$, a result due to C.H. Langford in 1927.

THEOREM 3. $\text{Th}(\mathfrak{N})$ is decidable.

PROOF. Let us enrich the structure $\mathfrak{N}$ by making 0 a distinguished element and adding the successor function $S(x) = x + 1$ (the element next to x in the ordering). Call the resulting structure $\mathfrak{N}_1 = \langle \omega, 0, \leq, S \rangle$ and denote the corresponding language by L_1 . We shall decide $\text{Th}(\mathfrak{N}_1)$, from which the decidability of $\text{Th}(\mathfrak{N})$ follows.

Let us use the abbreviation $S^n(t)$ to denote n applications of S to the term t , thus $S^3(x) = S(S(S(x)))$. In particular, $S^0(y) = y$. The terms of the language are $0, x, y, \dots, S^n(0), S^n(x), \dots, 1 \leq n$.

The class $\mathcal{R}$ of formulas to which we shall reduce every formula of L_1 will be the following

(1) $t_1 = t_2, t_1 < t_2$, where t_1, t_2 are terms;

(2) formulas which are disjunction of conjunctions of formulas in (1).

For example $[S^3(0) = x \wedge S(y) < z] \vee S^5(z) < S^3(y)$ is in $\mathcal{R}$.

We shall show that every formula A of L_1 is equivalent in $\mathfrak{N}_1$ to a formula $B \in \mathcal{R}$. Our proof will also provide a method for effectively transforming A into B .

The statement that two formulas C and D are equivalent in $\mathfrak{N}_1$ means that $\mathfrak{N}_1 \models C \leftrightarrow D$. We shall make assertions concerning equivalence of formulas leaving verification to the reader.

Let A be an open, i.e. quantifier-free formula. Express all other propositional connectives by means of $\vee, \wedge, \neg$. Move all occurrences of $\neg$ next to the atomic formulas, using rules such as $\neg[C \vee D] \equiv \neg C \wedge \neg D$. Drop all occurrences of double-negation $\neg\neg$. Replace constituents of the form $t_1 \leq t_2$ by $t_1 = t_2 \vee t_1 < t_2$, $\neg t_1 = t_2$ by $t_1 < t_2 \vee t_2 < t_1$, and $\neg t_1 < t_2$ by $t_1 = t_2 \vee t_2 < t_1$. Finally, by use of the distributive law for $\wedge$ and $\vee$, transform the formula into a formula in $\mathcal{R}$. Thus we see that repeated applications of the above rules will transform any open formula into an equivalent formula in $\mathcal{R}$.

Assume now that A_1 has the form $\exists y (C_1 \vee \dots \vee C_n)$ where each C_i is a conjunction of formulas $t_1 = t_2$ or $t_1 < t_2$. We have $A_1 \equiv \exists y C_1 \vee \dots \vee \exists y C_n$. Thus it suffices to give rules for transforming a formula of the form

$$A_1 = \exists y [t_1 = t_2 \wedge \dots \wedge t_{2i-1} = t_{2i} \wedge \\ t_{2i+1} < t_{2i+2} \wedge \dots \wedge t_{2k-1} < t_{2k}].$$

The reader can work out for himself how to treat the case that some

equation or inequality in A_1 is of the form $S^m(y) = S^i(y)$ or $S^m(y) < S^i(y)$. Thus we may assume that in each equation or inequality in A_1 at most one side is of the form $S^i(y)$.

For any terms t_1, t_2 , and $1 \leq n$, $\mathfrak{N}_1 \models t_1 < t_2 \leftrightarrow S^n(t_1) < S^n(t_2)$ and similarly for $t_1 = t_2$. By applying to both sides of all equations and inequalities in A_1 appropriate powers S^i , we transform A_1 into an equivalent formula in which all occurrences of y are of the form $S^m(y)$, with the same $1 < m$. Let us assume A_1 already has this property. "Eliminate" $\exists y$ from A_1 by: (1) dropping $\exists y$ from A_1 ; (2) for each conjunct $S^m(y) = t_j$ add a conjunct $S^{m-1}(0) < t_j$; (3) for each $S^m(y) < t_j$ add $S^m(0) < t_j$; (4) if any equation $S^m(y) = t_j$ occurs in A_1 , replace all occurrences of $S^m(y)$ in A_1 by t_j ; (5) assuming that no such equations occur and that all inequalities are of the form $S^m(y) < t_j$, or all are of the form $t_j < S^m(y)$, drop all conjuncts involving $S^m(y)$; (6) lastly, if no equation involving $S^m(y)$ occurs but inequalities of both types do appear, then for every pair $t_j < S^m(y)$ and $S^m(y) < t_p$ add a conjunct $S(t_j) < t_p$, and later drop all conjuncts involving $S^m(y)$. It is clear that steps (1)–(6) transform A_1 into an equivalent formula $B \in \mathcal{R}$ which does not contain y .

Let A be any formula of L_1 . Since $\forall x F \equiv \neg \exists x \neg F$, we may assume that A contains just existential quantifiers, say n in number. Let $\exists y D$ be an innermost occurrence of $\exists$, i.e. D is open. Transform D into a disjunction of conjunctions as explained before. Then $\exists y D \equiv A_1$ where A_1 has the form treated above. Distribute $\exists y$ over the disjunctions, and treat each disjunct by steps (1)–(6). By these transformations $\exists y D$ is replaced in A by an equivalent open formula, and A is transformed into an equivalent formula with $n - 1$ quantifiers. Repeating this process n times, A will be effectively transformed into a $B \in \mathcal{R}$.

Finally, if A was a sentence, then the transformed formula is a sentence, hence a propositional combination of formulas $S^m(0) = S^i(0)$ or $S^m(0) < S^i(0)$. The truth or falsehood of such a sentence can be directly ascertained. Thus we have a decision procedure for $\text{Th}(\mathfrak{N}_1)$ and hence for $\text{Th}(\mathfrak{N})$. $\square$

Let us observe that we could have avoided the passage from $\mathfrak{N}$ to $\mathfrak{N}_1$, and this because the relation $y = S^n(x)$ is definable by an appropriate formula $D_n(x, y)$ in $\mathfrak{N}$. This enables us to translate all basic formulas $t_1 < t_2$ and $t_1 = t_2$ into formulas of N , and thus get a reduction class of formulas of $\mathfrak{N}$.

Note that if we carry out the quantifier-elimination procedure in $\mathfrak{N}$ then we actually do not get rid of all quantifiers. Rather, we "hide" them in the formulas $D_n(x, y)$. But this still yields the desired results. In general, the elimination of quantifiers method should be construed in this broader sense.

The same decision procedure applies to $\text{Th}(\text{DO})$. The only modification required is that the various statements concerning equivalence of formulas which were mathematically verified for $\mathfrak{N}_1$, must now be derived as formal consequences of the axioms DO. Following this route, we not only decide $\text{Th}(\text{DO})$ but also show that $\text{Th}(\text{DO}) = \text{Th}(\mathfrak{N})$, i.e. $\text{Th}(\text{DO})$ is complete.

1.3. Presburger's arithmetic

The theory PAR was decided by PRESBURGER [1929] using the method of elimination of quantifiers. By an appropriate formula $x <_n y$ we can express, for each fixed n , the relation $x < y \wedge x \equiv y \pmod{n}$. Thus, for example, $x <_3 y$ is $\exists z [\neg z = 0 \wedge x + z + z + z = y]$. Enrich the structure $\langle \omega, + \rangle$ by making 0, 1 into distinguished elements. The terms of the language are now 0, 1, $x, y, \dots$, and all expressions which are sums of these, e.g. $x + z + z + 1 + 1 + 1$ abbreviated by $x + 2z + 3$.

The reduction set $\mathcal{K}$ will consist of all formulas obtained from the basic formulas $t_1 = t_2$, $t_1 <_n t_2$ (t_1, t_2 are terms, n is an integer) by conjunctions and disjunctions. The proof, while not trivial, is not too hard and follows the lines of the proof of 1.2.

1.4 Theory of real numbers

This is perhaps the best known application of the elimination of quantifiers method. We consider the field of real numbers $\mathfrak{R} = \langle \mathbb{R}, 0, 1, +, \cdot, \leq \rangle$ as an ordered field. Instead of giving Tarski's original decision procedure we shall outline the algorithm of COHEN [1969] using the formulation in Monk's thesis.

We introduce, on a provisional basis, certain algebraic-like functions. Let $P(x_1, \dots, x_n) \in Z[x_1, \dots, x_n]$ be a polynomial with integral coefficients, $d_n(P)$ be its degree in x_n , and let $\eta \in \mathbb{R}^{n-1}$. Define $P_\eta(x_n) = P(\eta_1, \dots, \eta_{n-1}, x_n)$. For $1 \leq i \leq d_n(P)$ define $f_{P,i}(\eta)$ to equal 0 if $P_\eta \equiv 0$ or P has no real roots, otherwise the i -th real root of $P_\eta = 0$ if there are at least i such roots, otherwise the largest real root. This makes $f_{P,i}(x_1, \dots, x_n)$ a term which denotes the function $f_{P,i} : \mathbb{R}^{n-1} \rightarrow \mathbb{R}$. Call such terms algebraic functions.

A polynomial relation is a Boolean combination of atomic formulas of the form $0 \leq P$, where $P \in Z[x_1, \dots, x_n]$. An algebraic relation is a Boolean combination of polynomial relations and formulas of the forms, $0 \leq P[x_1, \dots, x_{n-1}, f_1(x_1, \dots, x_{n-1})]$, or $f_1 \leq f_2$, where $P \in Z[x_1, \dots, x_n]$ and f_1, f_2 are algebraic functions. With each algebraic relation a *rank* is associated in such a way that the rank of a polynomial relation is 0.

The procedure for the elimination of quantifiers will reduce any formula

of the original language to an open formula (i.e. polynomial relation) and this by passing temporarily through the more general algebraic relations.

The proof involves two lemmas. The first lemma asserts that a formula $\exists x_n A$, where A is a polynomial relation, is equivalent to an algebraic relation B . The second lemma states that an algebraic relation B of rank $1 \leq k$ is equivalent to an algebraic relation of rank at most $k - 1$. This lemma implies by induction that every algebraic relation is equivalent to a polynomial relation. Taken together, these facts ensure that every formula is equivalent to an open formula.

The proofs of the lemmas make use of Rolle's theorem to the effect that between every two consecutive roots of $p(x) = 0$ there lies a root of $p'(x) = 0$. If $p(x)$ is a polynomial, then the location of the roots of $p(x) = 0$ can be determined, with sufficient accuracy for our purposes, from the location of roots of $p'(x) = 0$ and the values $p(-\infty)$, $p(+\infty)$. Denote, for $P \in Z[x_1, \dots, x_n]$, $P' = \partial P / \partial x_n$. It turns out, roughly speaking, that statements involving $f_{P,i}$, i.e. statements about the i -th root of $P = 0$, can be transformed into statements involving the terms $f_{P',j}$. Within the framework of our notion of rank, this entails rank reduction which is the key point in the proof of the second lemma.

1.5. Other theories

Let us briefly mention some additional theories which we have shown decidable by the method of elimination of quantifiers.

Let $\mathbb{Q}$ be the rational numbers, $\eta = \langle \mathbb{Q}, \leq \rangle$ their order-type. $\text{Th}(\eta)$ is decidable.

Let ALC be the class of algebraically closed fields, then $\text{Th}(\text{ALC})$ is decidable. Here every formula is equivalent to an open formula, a fact that can be established, for example, by employing the classical algebraic elimination theory.

If BA is the class of all Boolean algebras, then $\text{Th}(\text{BA})$ is decidable. This result is due to TARSKI [1949] and is somewhat difficult.

2. Model theoretic methods

2.1. Categoricity, completeness and decidability

A theory T is called *categorical* in cardinality α if all models $\mathfrak{A} \models T$ of cardinality $c(\mathfrak{A}) = \alpha$ are pairwise isomorphic. By the cardinality of $\mathfrak{A}$ we mean the cardinality of the domain of $\mathfrak{A}$. The following simple observation is due to R. Vaught. It is assumed that T is countable.

THEOREM 4. *If the theory T has no finite models and is categorical in some (necessarily infinite) cardinality α then T is complete.*

PROOF. Assume, by way of contradiction, that T is not complete. Then there exists a sentence S in the language of T such that $T_1 = T \cup \{S\}$ and $T_2 = T \cup \{\neg S\}$ are consistent. Hence there are countable (i.e. finite or denumerable) models $T_1 \models \mathfrak{A}_1$, $T_2 \models \mathfrak{A}_2$. Since T has no finite models, $c(\mathfrak{A}_1) = c(\mathfrak{A}_2) = \omega$. If $\alpha = \omega$, then $\mathfrak{A}_1 \approx \mathfrak{A}_2$, but $\mathfrak{A}_1 \models S$ and $\mathfrak{A}_2 \models \neg S$, a contradiction. Otherwise there exist, by the Skolem–Tarski–Vaught theorem, elementary extensions $\mathfrak{A}_1 < \mathfrak{B}_1$, $\mathfrak{A}_2 < \mathfrak{B}_2$ so that $c(\mathfrak{B}_1) = c(\mathfrak{B}_2) = \alpha$. Again $\mathfrak{B}_1 \approx \mathfrak{B}_2$, $\mathfrak{B}_1 \models S$ and $\mathfrak{B}_2 \models \neg S$. $\square$

The stipulation that T has no finite models is essential. Consider the theory E of just equality $=$. E is categorical in every cardinality. Yet $E \cup \{\forall x \forall y [x = y]\}$, as well as $E \cup \{\exists x \exists y [\neg x = y]\}$, are consistent.

Perhaps the simplest application is proving that $\text{Th}(\eta)$ is decidable. Consider the axioms DNO consisting of the axioms for total-order together with

$$\forall x \forall y \exists z [x < y \rightarrow x < z < y]$$

$$\forall x \exists y \exists z [z < x < y].$$

Every model $\langle A, \leq \rangle \models \text{DNO}$ is a totally and densely ordered set without a first or last element. By Cantor's characterization of the order type $\eta = \langle \mathbb{Q}, \leq \rangle$, if $c(A) = \omega$ then $\eta \approx \langle A, \leq \rangle$. Consequently, $\text{Th}(\text{DNO})$ is complete and hence, by Theorem 1, decidable. Now $\eta \models \text{DNO}$ so that $\text{Th}(\text{DNO}) \subseteq \text{Th}(\eta)$, but $\text{Th}(\text{DNO})$ is complete so that $\text{Th}(\text{DNO}) = \text{Th}(\eta)$. $\square$

2.2. Algebraically closed fields

Next we consider the theory ALC of algebraically closed fields. This theory can be axiomatized in a language L having symbols $0, 1, +, \cdot$, by writing the usual field axioms and adding a sequence of axioms A_n , $n = 1, 2, \dots$,

$$A_n = \forall y_0 \cdots y_{n-1} \exists x [y_0 + y_1 x + \cdots + y_{n-1} x^{n-1} + x^n = 0].$$

The axiom A_n is written using some obvious abbreviations.

The axioms ALC are not complete because the characteristic of the field has not been specified. This can be done by adding, for a prime p , an axiom $C_p = p \cdot 1 = 0$, where the left-hand side abbreviates a sum of terms 1 . To obtain axioms for characteristic 0 put $C_0 = \{\neg C_2, \neg C_3, \dots\}$.

We shall now show that $T_p = \text{ALC} \cup \{C_p\}$ is complete for any prime p , and $T_0 = \text{ALC} \cup C_0$ is also complete. Let $F \models T_p$, where p is a prime or $p = 0$, be an algebraically-closed field of characteristic p and cardinality $\omega < c(F) = \alpha$. Let $P \subset F$ be the prime-field in F , then $P = \mathbb{Z}/p\mathbb{Z}$ for $p \neq 0$, and $P = \mathbb{Q}$ if $p = 0$. By Steinitz's structure theorem for algebraically-closed fields, there exists a set $X \subseteq F$ of elements algebraically independent over P so that $F \supset P(X) \supset P$ is the algebraic closure of $P(X)$. The isomorphism type of F depends just on P (i.e. p) and $c(X)$, the so-called degree of transcendence of F . Now if $\omega < c(F)$ then $c(X) = c(F) = \alpha$. Hence for all p , T_p is categorical in every non-countable cardinality $\omega < \alpha$.

By use of Theorem 1, this implies that for each $p \geq 0$, the theory T_p of algebraically-closed fields of characteristic P is decidable.

Since $\text{ALC} \cup C_0$, $\text{ALC} \cup \{C_p\}$, p prime, gives an enumeration of all completions of ALC , it follows from Theorem 2 that $\text{Th}(\text{ALC})$, the theory of algebraically-closed fields is decidable.

2.3. Real-closed fields

Tarski's result concerning the decidability of the theory of the field of real numbers can also be achieved by model theoretic methods. We first need a set of axioms for the field of real numbers. These were provided by Artin and Schreier in their famous study of real-closed fields.

Consider a language L_1 which, like L of Section 2.2, has $0, 1, +, \cdot$, but in addition has a greater or equal symbol $\leq$. The axioms RLC consist of the following: the field axioms, axioms stating that $\leq$ is a total order, and furthermore

$$\forall x \forall y \forall z [x \leq y \wedge 0 \leq z \rightarrow xz \leq yz],$$

$$\forall x \forall y \forall z [x \leq y \rightarrow x + z \leq y + z],$$

$$\forall x \exists y [0 \leq x \rightarrow y^2 = x],$$

$$A_n \quad \text{for } n = 1, 3, 5, \dots$$

Here, as in 2.2, A_n is the statement that the n -th degree polynomial equation has a root.

The field of real numbers is a model of RLC but by no means the only model. Any ordered field $\langle F, 0, 1, +, \cdot, \leq \rangle \models \text{RLC}$ will be called (*ordered*) *real-closed*. $\text{Th}(\text{RLC})$ is not categorical in any power, so that Vaught's test cannot be used. Completeness, and consequently decidability, are proved by means of Robinson's concept of model completeness.

A theory T is *model complete* if for any two models $T \models \mathfrak{A}$, $T \models \mathfrak{B}$ such that $\mathfrak{A} \subseteq \mathfrak{B}$, we have $\mathfrak{A} < \mathfrak{B}$ ($\mathfrak{B}$ is an elementary extension of $\mathfrak{A}$).

ROBINSON [1956] gave a test for model completeness. From this test the model completeness of RLC can be deduced. The proof, while not very hard, does require some effort. Alternatively one can use the following test.

T is model complete if for any two models $\mathfrak{A} \subseteq \mathfrak{B}$ of T there exists an elementary extension $\mathfrak{A} < \mathfrak{C}$ such that $\mathfrak{B} \subseteq \mathfrak{C}$. Combining this with algebraic properties of real-closed fields and with the method of ultraproducts we can get a somewhat different proof for the model completeness of $\text{Th}(\text{RLC})$.

Now a model complete theory T need not be complete. However, if T is model complete and has a *prime model* P which is, up to isomorphism, included as a submodel in every model of T , then T is complete. It is readily seen that under these conditions every two models of T are elementarily equivalent.

The theory $\text{Th}(\text{RLC})$ has a prime model. Namely, every real-closed field F is of characteristic 0 and hence contains the field Q of rational numbers. It therefore also contains an isomorphic copy of the field of real-algebraic numbers and this is the common prime field. Consequently $\text{Th}(\text{RLC})$ is complete and decidable. The field $\mathfrak{R}$ of real numbers satisfies $\mathfrak{R} \models \text{RLC}$, hence $\text{Th}(\mathfrak{R}) = \text{Th}(\text{RLC})$ and is decidable.

It should be remarked that this approach to the decidability of the field of real numbers is, despite the difference in methods, not too different from the classical elimination of quantifiers method. At the bottom of the proof of model completeness lies the fact that if two ordered fields F_1, F_2 are isomorphic (the mapping preserves also the order) then their real-closures are isomorphic. This is proved by using information concerning the location of roots of equations. The analysis involved is not too different from the examination of the location of roots in the elimination of quantifiers method. On the other hand, one can claim that the uniqueness of the real-closure is a basic algebraic result established on its own right. In the model-theoretic proof of the decidability of $\text{Th}(\text{RLC})$ we are thus quoting a standard result, and from this point of view the proof is more elementary.

2.4. Theory of DO revisited

By way of illustrating how model-theoretic methods are useful for establishing decidability even in the absence of categoricity, let us re-examine $\text{Th}(\text{DO})$.

In 1.1, Example 2, we observed that every model of DO has the order-type $\omega + (\omega^* + \omega)\lambda$. We shall show that every countable model

$\mathfrak{A} = \{A, \leq\} \models \text{DO}$ has an elementary extension $\mathfrak{A} < \mathfrak{B}$ for which the λ is η . This will imply $\text{Th}(\mathfrak{A}) = \text{Th}(\mathfrak{B})$, hence every two countable models of DO are elementarily equivalent, and hence $\text{Th}(\text{DO})$ is complete and decidable.

Define an equivalence relation E on any model $\mathfrak{A} \models \text{DO}$. $xEy \equiv c(\{z \mid x < z < y \vee y < z < x\}) < \omega$, i.e. the number of elements between x and y is finite. We see that the equivalence classes with respect to E are the “blocks” ω , and each $\omega^* + \omega$, in the order type $\omega + (\omega^* + \omega)\lambda$ of $\mathfrak{A}$. Consider any two blocks (equivalence classes) B_1, B_2 of $\mathfrak{A}$, without loss of generality let $x < y$ for all $x \in B_1, y \in B_2$. It is consistent with all the elementary statements about $\mathfrak{A}$, i.e. with the complete diagram $\text{CD}(\mathfrak{A})$ of $\mathfrak{A}$, to assume the existence of an element c such that $x < c < y$ for all $x \in B_1, y \in B_2$. Thus $\text{CD}(\mathfrak{A})$ and all these inequalities have a countable model $\mathfrak{A}_1$ which is an elementary extension $\mathfrak{A} < \mathfrak{A}_1$ of $\mathfrak{A}$. In this $\mathfrak{A}_1$ the block B of c lies between B_1 and B_2 . Similarly we can construct an extension with a block above B_2 . Because the extension $\mathfrak{A} < \mathfrak{A}_1$ is countable, it is possible to construct a tower of elementary extensions $\mathfrak{A} < \mathfrak{A}_1 < \dots$, so that each $\mathfrak{A}_n$ is countable and for each pair B_1, B_2 of blocks of each $\mathfrak{A}_n$ there exists an $n < k$ and a block B of $\mathfrak{A}_k$ situated between B_1 and B_2 , and similarly for a block above B_2 . Let $\mathfrak{B} = \bigcup_{n < \omega} \mathfrak{A}_n$, then $\mathfrak{A} < \mathfrak{B}$, $\mathfrak{B}$ is countable, and the blocks of $\mathfrak{B}$ are densely ordered. Thus the order type of $\mathfrak{B}$ is $\omega + (\omega^* + \omega)\eta$, which completes the proof.

2.5. Further results

Many additional important results we obtained by model-theoretic methods, sometimes in combination with the method of elimination of quantifiers. Let us mention without proofs a few outstanding theorems. The proofs usually involve deep mathematical results concerning the structures in question, making for an interesting combination of standard mathematics and logic.

THEOREM 5 (AX and KOCHEN [1965a, 1965b, 1966]). *The theory of p -adic fields is decidable.*

This result laid to rest a long-standing conjecture that the only decidable fields are the real-closed and the algebraically closed fields.

THEOREM 6 (AX [1968]). *The theory of the class of all finite fields is decidable.*

THEOREM 7 (SZMIELEW [1954]). *The theory of commutative groups is decidable.*

THEOREM 8 (EHRENFEUCHT [1959]). *The theory of linearly (totally) ordered sets is decidable.*

This result was announced in an abstract. The first full proof to be published is due to LÄUCHLI and LEONARD [1966]. As will be seen in the next chapter, this result is an easy consequence of the method in RABIN [1969].

Finally we shall quote a special case of more general results relating models to decidability.

Let $\mathfrak{A} = \langle A, f_0, \dots, f_i, \dots \rangle_{i < \alpha}$ and $\mathfrak{B} = \langle B, g_0, \dots, g_i, \dots \rangle_{i < \alpha}$, $\alpha \leq \omega$, be similar algebras of the same type, i.e. f_i and g_i are n_i -ary operations on $\mathfrak{A}$ and $\mathfrak{B}$ respectively. The direct product $\mathfrak{A} \times \mathfrak{B}$ is defined in the obvious manner.

THEOREM 9. *If $\text{Th}(\mathfrak{A})$ and $\text{Th}(\mathfrak{B})$ are decidable so is $\text{Th}(\mathfrak{A} \times \mathfrak{B})$.*

This is but a special case of a general study of the first-order properties of products of structures and classes of structures initiated by MOSTOWSKI [1952] and developed by FEFERMAN and VAUGHT [1959]. We have restricted ourselves to a very special case in order to avoid the elaborate definitions appearing in the general theory.

The method of products is a powerful tool for obtaining new decidability results from known ones. The following example is due to Mostowski. We know that $\text{Th}(\langle \omega, + \rangle)$ is decidable, see Section 1.3. From the theory of general products it follows that the direct sum $\mathfrak{B}$ of ω copies of $\langle \omega, + \rangle$ has a decidable theory. The domain of P consists of all ω -length vectors

$$v = (n_0, \dots, n_k, 0, 0, \dots), \quad n_i \in \omega, \quad k = 0, 1, \dots,$$

and the operation is component-wise addition. Define a mapping $\phi(v) = p_0^{n_0} \cdots p_k^{n_k}$, where p_i is the $(i+1)$ -th prime. The mapping ϕ is an isomorphism $\phi: \mathfrak{B} \rightarrow \langle \omega - \{0\}, \cdot \rangle = \mathfrak{M}$ onto the multiplicative semi-group of integers. Hence $\text{Th}(\mathfrak{M})$ is decidable, a result due to Skolem.

3. The method of interpretations

3.1. Semantic interpretations

We shall start by outlining what is meant by obtaining a structure $\mathfrak{A} = \langle A, R \rangle$ from a structure $\mathfrak{B} = \langle B, S_1, S_2, \dots \rangle$ by means of definable relations. We need some preliminary notions. Let L be the language of $\mathfrak{A}$

and L_1 be the language of $\mathfrak{B}$. Let $D(x, y, \dots)$ be a formula of L_1 with x as a free variable but possibly containing other free variables $y, \dots$, which will play the role of parameters. Abbreviate $D(x, y, \dots)$ by $D(x)$ or even D .

If F is a formula of L_1 , then the formula F^D obtained from F by *relativizing* all quantifiers of F to D , is defined inductively on the structure of F by the following rules. If F is quantifier-free then $F^D = F$. If $F = E \vee G$ or $F = \neg E$ then $D^D = E^D \vee G^D$ or $F^D = \neg E^D$, respectively. The crucial cases are $F = \exists u G$ and $F = \forall u G$:

$$(\exists u G)^D = \exists u [D(u) \wedge G^D], \quad (\forall u G)^D = \forall u [D(u) \rightarrow G^D].$$

Here $D(u)$ means $D(u, y, \dots)$, i.e. u substituted for x in D . Note that in order to correctly effect the relativization, we must sometimes alphabetically change the names of certain variables in F in order to avoid binding a variable other than x , which is free in D .

Let $b \in B, \dots$, be a sequence of values in B for the parameters $y, \dots$, of D . Define $C = \{a \mid \mathfrak{B} \models D(a, b, \dots)\}$. This is the domain defined by D and the specialization $y = b, \dots$ of the parameters. The subset $C \subseteq B$ induces a substructure $\mathfrak{C} = \langle C, S_1 \upharpoonright C, S_2 \upharpoonright C, \dots \rangle$ of $\mathfrak{B}$.

LEMMA. *Let $F(z_1, \dots, z_n)$ be a formula of L_1 , and let $D, B, b \in B, \dots$, and C be as above, then for $c_1, \dots, c_n \in C$*

$$\mathfrak{B} \models F^D(c_1, \dots, c_n) \quad \text{iff} \quad \mathfrak{C} \models F(c_1, \dots, c_n).$$

Thus the effect of relativization is to convert satisfaction of the formula F in $\mathfrak{B}$ to satisfaction in the substructure $\mathfrak{C}$.

A somewhat more complex construction is the following. For the sake of the simplicity of the notation, let us restrict ourselves to a formula $D(x)$ of L_1 containing just the free variable x (and no parameters) and a formula $E(u, v)$ with two free variables.

DEFINITION 3. The structure $\mathfrak{B}(D, E) = \langle C, R \rangle$ induced in $\mathfrak{B}$ by $D(x)$ and $E(u, v)$ has, by definition, the domain $C = \{c \mid \mathfrak{B} \models D(c)\}$ and the binary relation $R \subseteq C \times C$, $R = \{(b, c) \mid b, c \in C, \mathfrak{B} \models E(b, c)\}$.

Let now $F(z_1, \dots, z_n)$ be a formula in a language with a binary predicate symbol P and define $F^{D, E}$ to be the formula obtained from F by *first* forming F^D and *then* replacing in F^D all atomic formulas $P(z_1, z_2)$ by $E(z_1, z_2)$. Note that the quantifiers in $E(u, v)$ are not being relativized to D . The following lemma is actually a corollary of the previous lemma. It relates satisfaction in the induced structure to satisfaction in $\mathfrak{B}$.

LEMMA. For $c_1, \dots, c_n \in C$,

$$\mathfrak{B}(D, E) \models F(c_1, \dots, c_n) \quad \text{iff} \quad \mathfrak{B} \models F^{D, E}(c_1, \dots, c_n).$$

The application to decidability rests on the following theorem taken from RABIN [1965].

Let T and T_1 be theories in the languages L and L_1 , respectively, and let $\mathcal{K}$ and $\mathcal{K}_1$ be classes of structures such that $T = \text{Th}(\mathcal{K})$, $T_1 = \text{Th}(\mathcal{K}_1)$. Assume that L has the predicate symbols $P_0, \dots, P_k$ and no operation symbols.

THEOREM 10. Let $D(x, y, \dots)$ be a formula of L_1 , and $E = (E_0, \dots, E_k)$ be a sequence of formulas so that if P_i is n_i -ary then E_i has n_i free variables, $0 \leq i \leq k$.

Assume that (1) For all $\mathfrak{B} \in \mathcal{K}_1$ and all values $y = b, \dots$ of the parameters of D , $\mathfrak{B}(D, E) \models T$. (2) For every $\mathfrak{A} = \langle A, R_0, \dots, R_k \rangle \in \mathcal{K}$, there exists a model $\mathfrak{B} \in \mathcal{K}_1$ and a specialization $y = b \in B, \dots$ such that for this specialization $\mathfrak{A} \approx B(D, E)$.

Under these conditions, if T_1 is decidable then so is T . Conversely, if T is undecidable then so is T_1 .

PROOF. Let F be a sentence of L , put $G = \forall y \dots F^{D, E}$ where the universal quantification is over all the parameter-variables in $D(x, y, \dots)$ (these variables are free in F , if F did contain quantifiers). By the second lemma, for any $\mathfrak{B} \in \mathcal{K}_1$ and specialization $y = b \in B \dots$

$$(*) \quad \mathfrak{B} \models F^{D, E}(b, \dots) \quad \text{iff} \quad \mathfrak{B}(D, E) \models F.$$

Let now $F \in T$. Condition (1) implies $\mathfrak{B}(D, E) \models F$ for any $\mathfrak{B} \in \mathcal{K}_1$, $y = b, \dots$. Hence the left side of $(*)$ holds, hence $\mathfrak{B} \models G$. But $\mathfrak{B} \in \mathcal{K}_1$ was arbitrary, hence $G \in \text{Th}(\mathcal{K}_1) = T_1$.

Next assume $G \in T_1$. Let $\mathfrak{A} \in \mathcal{K}$, then, by (2), for some $B \in \mathcal{K}$ and $y = b, \dots$, $\mathfrak{A} \approx \mathfrak{B}(D, E)$. We have $\mathfrak{B} \models G$, hence $\mathfrak{B} \models F^{D, E}(b, \dots)$. Therefore, by $(*)$, $\mathfrak{B}(D, E) \models F$, hence $\mathfrak{A} \models F$; consequently $\mathcal{K} \models F$ and $F \in T$.

Let T_1 be decidable and F be any sentence of L . Form G ; since $G \in T_1$ iff $F \in T$, we can determine whether $F \in T$. $\square$

Remark. It is readily seen that if T is finitely axiomatizable then condition (1) can be dispensed with by modifying the construction of G .

We have stated Theorem 10 for first-order languages. With appropriate changes it also holds if L_1 or even both L and L_1 are second-order

languages. The only case of second-order languages which is of any interest from the point of view of decidability is that of monadic second-order languages which have variables ranging over *subsets* of the domain but no variables ranging over relations on the domain. This is because once we have a variable ranging over, say, binary relations, the theory of all true sentences of the second-order language is undecidable.

Assume that L_1 has set variables $A, B, \dots$. Then the relativizing formula $D(x)$ may be of the form $x \in A$ and A will be a parameter in $F^{D,E}$. If L has set variables then they must also be relativized to D by rules such as

$$(\forall A F)^D = \forall A [\forall x [x \in A \rightarrow D(x)] \rightarrow F^D].$$

With these natural modifications, Theorem 10 holds for monadic second-order languages.

3.2. Decidable second-order theories

Let us consider monadic second-order languages L_1 which have set variables $A, B, \dots$, and the $\in$ relation. To be appropriate for a structure $\mathfrak{A} = \langle A, R \rangle$ where R is, say, a binary relation, L_1 must also have a binary predicate symbol P . For such a language L_1 the (*monadic*) *second-order* theory $\text{Th}_2(\mathfrak{A})$ of $\mathfrak{A}$ is the set of all sentences of L_1 true in $\mathfrak{A}$. Similarly we define $\text{Th}_2(\mathcal{K})$ for a class $\mathcal{K}$ of similar structures by $\text{Th}_2(\mathcal{K}) = \bigcap_{\mathfrak{A} \in \mathcal{K}} \text{Th}_2(\mathfrak{A})$.

The first significant results of second-order decidability, beyond the decidability of just pure monadic second-order logic, deal with the decidability of $\text{Th}_2(\langle \omega, S \rangle)$ where $S(x) = x + 1$ is the successor function.

THEOREM 11 (BÜCHI [1962]). $\text{Th}_2(\langle \omega, S \rangle)$ is *decidable*.

This result was actually preceded by a weaker version. Consider a *weak* monadic second-order language LW which has set variables $\alpha, \beta, \dots$ which are restricted to range over *finite* subsets of the domain. The theory of a structure $\mathfrak{A}$ in the language LW , will be called the *weak* (monadic) second-order theory of $\mathfrak{A}$ and denoted by $\text{Th}_w(\mathfrak{A})$.

BÜCHI [1960] and ELGOT [1961] have proved that $\text{Th}_w(\langle \omega, S \rangle)$ is decidable.

For future reference, denote $\text{Th}_2(\omega, S) = \text{S1S}$ (the second-order theory of one successor function) and $\text{Th}_w(\langle \omega, S \rangle) = \text{WS1S}$.

We cannot enter into details of these decidability proofs. Let us just say that they utilize methods and results of automata theory. The case of WS1S

employs concepts and results from theory of automata operating on finite sequences and is very simple and transparent. The proof of decidability of S1S required a new notion of an automaton operating on an infinite ω -sequence.

3.3. The tree theorem

Most of the proofs of decidability by interpretations involve the *Tree Theorem* due to Rabin [1969].

Let $T = \{0, 1\}^*$ be the set of all finite words (sequences) $x = x_1x_2 \cdots x_n$, $x_i \in \{0, 1\}$ on the alphabet $\{0, 1\}$. The empty sequence Λ is also in $\{0, 1\}^*$. The set T can also be interpreted as the infinite binary tree (see Fig. 1). Arbitrarily assigning 0 to *left* and 1 to *right*, the correspondence between node of the tree and T is as follows. The root corresponds to Λ ; the right successor (son) corresponds to 1, and the left successor to 0; the left successor of 1 is 10, etc.

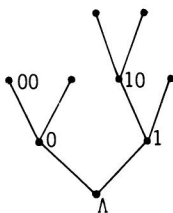


Fig. 1.

Thus we have on T the two *successor functions* $r_0(x) = x0$, $r_1(x) = x1$, $x \in T$. Let L_1 be an appropriate monadic second-order language having operation symbols r_0, r_1 . The set of all sentences of L_1 true in $\langle T, r_0, r_1 \rangle$ will be denoted, as usual, by $\text{Th}_2(\langle T, r_0, r_1 \rangle)$.

THEOREM 12 (Tree Decidability Theorem). *The second-order theory of two successor functions $\text{S2S} = \text{Th}_2(\langle T, r_0, r_1 \rangle)$ is decidable.*

The proof of this theorem requires a far-reaching extension of the theory of automata to cover the case of a finite automaton operating on an infinite tree. One interesting feature of the proof is that even though we want to establish certain facts concerning finite objects, namely the finite automata, transfinite induction over ordinals up to the first uncountable cardinal ω_1 is used in an essential way.

3.4. Presburger's arithmetic revisited

Büchi and Elgot used the decidability of WS1S to prove the decidability of PAR.

The key idea is to use finite sets $\alpha \subset \omega$ to code integers. Let χ_α be the characteristic function of α . Define

$$n(\alpha) = 1 \cdot \chi_\alpha(0) + 2 \cdot \chi_\alpha(1) + \cdots + 2^x \cdot \chi_\alpha(x) + \cdots.$$

We shall construct a formula $A(\alpha, \beta, \gamma)$ in the language of WS1S which will be true in $\langle \omega, S \rangle$ for $\alpha, \beta, \gamma \in \omega$ if and only if $n(\alpha) + n(\beta) = n(\gamma)$. This is done by considering the sequence χ_s of carriers in the addition of $n(\beta)$ to $n(\alpha)$ as binary numbers.

$$\begin{aligned} A(\alpha, \beta, \gamma) = & \exists \delta \forall x [\neg 0 \in \delta \wedge \\ & [S(x) \in \delta \leftrightarrow x \in \alpha \wedge x \in \beta \vee x \in \alpha \wedge \\ & x \in \delta \vee x \in \beta \wedge x \in \delta] \wedge [x \in \gamma \leftrightarrow \\ & x \in \alpha \wedge x \in \beta \wedge x \in \delta \vee \\ & x \in \alpha \wedge \sim x \in \beta \wedge \sim x \in \delta \cdots]]. \end{aligned}$$

By systematic use of $A(\alpha, \beta, \gamma)$ to replace $a + b = c$ in a sentence F of PAR, a sentence G in the language of WS1S is obtained. We have $F \in \text{Th}(\langle \omega, + \rangle)$ iff $G \in \text{WS1S}$ so that we can decide whether F is true.

3.5. Second-order theory of linear order

Let K_ω^ω be the class of all totally ordered sets $\langle A, \leq \rangle \models \text{OR}$ with a countable domain, $c(A) \leq \omega$.

THEOREM 13 (RABIN [1969]). $\text{Th}_2(K_\omega^\omega)$ is decidable.

PROOF. We can define on T the partial-order $x \leq y$, x is an initial segment of y , by a formula $x \leq y$. Namely,

$$x \leq y = \forall A [x \in A \wedge \forall z [z \in A \rightarrow r_0(z) \in A \wedge r_1(z) \in A] \rightarrow y \in A].$$

Also the lexicographic order $x \leq y$ is definable

$$x \leq y = x \leq y \vee \exists z [r_0(z) \leq x \wedge r_1(z) \leq y].$$

The ordered set $\langle \{x1 \mid x \in T\}, \leq \rangle$ has order type η . Therefore for every countable ordered set $\langle A, \leq \rangle$ there exists a set $\bar{A} \subseteq T$ such that $\langle A, \leq \rangle \approx \langle \bar{A}, \leq \rangle$. Using the relativizing formula $D(x, A) = x \in A$ and replacing $\leq$

by $\leq$, we see that $\text{Th}_2(K_\omega^\omega)$ can be interpreted in S2S in the manner of Theorem 9. Hence $\text{Th}_2(K_\omega^\omega)$ is decidable. $\square$

As simple corollaries we get difficult classical results.

COROLLARY. *$\text{Th}(\text{OR})$, the theory of linearly ordered sets, is decidable.*

The Skolem–Löwenheim theorem implies that every $\langle A, \leq \rangle \models \text{OR}$ is elementarily equivalent to a $B \in K_\omega^\omega$. Hence $\text{Th}(\text{OR}) = \text{Th}(K_\omega^\omega)$. The latter theory is, of course, decidable.

The monadic second-order language is sufficiently powerful to express the fact that a set is well-ordered. Namely, the sentence

$$W = \forall A \forall x \exists y \forall z [x \in A \rightarrow y \in A \wedge [z \in A \rightarrow y \leq z]]$$

has the property that a linearly ordered set $\mathfrak{A}$ satisfies $\mathfrak{A} \models W$ if and only if $\mathfrak{A}$ is well-ordered. This immediately leads to

COROLLARY. *The monadic second-order theory of countable well-ordered sets is decidable.*

PROOF. For any sentence F we have $K_\omega^\omega \models W \rightarrow F$ if and only if F is true in all countable well-ordered sets. $\square$

Every well-ordered set $\langle B, \leq \rangle$ has a countable elementary submodel $\mathfrak{A} = \langle A, \leq \rangle < \langle B, \leq \rangle$. Hence the first-order theory of well-ordered sets is the same as the first-order theory of countable well-ordered sets which is decidable by the previous corollary. Thus the first-order theory of well-ordered sets is decidable, a result due to TARSKI and MOSTOWSKI [1949].

3.6. Decidability in topology

It is possible to define in S2S the notion of a *path* $A \subseteq T$ going from the root to infinity

$$\begin{aligned} \text{Path}(A) = & A \in A \wedge \forall x \forall y [x \in A \rightarrow [r_0(x) \in A \vee r_1(x) \in A] \wedge \\ & [y \leq x \rightarrow y \in A] \wedge \neg [r_0(x) \in A \wedge r_1(x) \in A]]. \end{aligned}$$

Consider $\{0, 1\}^\omega$ with the usual Tychonoff product topology. This is the well-known Cantor Discontinuum CD. For every point $p : \{0, 1\} \rightarrow \omega$, the set $A \subset T$ of all finite initial segments of p , is a path of T and this is a one-to-one correspondence. We can also reproduce in S2S the topology of CD.

Let $B \subseteq T$ be a set which is a union of paths, then the set of paths $A \subseteq B$ is a closed subset of CD , and this again is a one-to-one correspondence. Define

$$CL(B) = \forall x [x \in B \rightarrow \exists A [\text{Path}(A) \wedge A \subseteq B \wedge x \in A]].$$

THEOREM 14 (RABIN [1969]). *The monadic second-order theory of CD , with the set variables restricted to range over closed sets, is decidable.*

PROOF. Let F be any sentence in the language of CD . Relativize all individual variables to $\text{Path}(X)$ and all (closed) set variables to $CL(B)$, replace all formulas $x \in B$ of F by $X \subseteq B$. The resulting sentence E is true in $S2S$ if and only if $CD \models F$. $\square$

With slight changes, accounting for the fact that two different sequences $p, q \in \{0, 1\}^\omega$ may represent the same element of the real-line segment $[0, 1]$, the above proof may be modified to cover the case of $[0, 1]$.

3.7. Boolean algebras

The following theorem settles the decidability of $\text{Th}(BA)$ — the elementary theory of Boolean algebras and much more.

THEOREM 15 (RABIN [1969]). *Let $\mathfrak{B}_\omega$ be the free Boolean algebra on ω generators and let LI be a second-order language appropriate for Boolean algebras with set variables ranging over ideals of the algebras. $\text{Th}_I(\mathfrak{B}_\omega)$, the theory of $\mathfrak{B}_\omega$ in the language LI , is decidable.*

PROOF. The set of all closed-and-open (clopen) subsets of CD is a Boolean algebra isomorphic to $\mathfrak{B}_\omega$, hence we can identify it with $\mathfrak{B}_\omega$. If $I \subseteq \mathfrak{B}_\omega$ is any ideal then $U(I) = \bigcup_{S \in I} S$ is an open set $U(I) \subseteq CD$. The sets $U(I)$ run through all open sets of CD and the correspondence is 1–1. Furthermore, for $S \in \mathfrak{B}_\omega$, $S \subseteq U(I)$ if and only if $S \in I$.

Every sentence of LI can therefore be translated into a sentence about CD by relativizing the individual variables to set variables ranging over clopen subsets of CD , relativizing the ideal variables to variables ranging over open sets (i.e. complements of closed sets) of CD , and replacing $x \in I$ by $X \subseteq I$. The transformed sentence is true in CD if and only if the original sentence is true in $\text{Th}_I(\mathfrak{B}_\omega)$, and the former question is decidable. $\square$

Let now B be any countable Boolean algebra. Then there exists an ideal $J \subseteq \mathfrak{B}_\omega$ so that $\mathfrak{B} \approx B_\omega/J$, and the ideals $I \subseteq \mathfrak{B}$ are in a natural 1–1

correspondence with the ideal $J \subseteq J_1 \subseteq \mathfrak{B}_\omega$. By the method of interpretations, this will yield the following theorem. Denote by $\mathbf{BA}^\omega$ the class of all countable Boolean algebras.

THEOREM 16. $\text{Th}_1(\mathbf{BA}_\omega)$, the theory in the language LI of all countable Boolean algebras, is decidable.

If we restrict ourselves to sentences $G = \forall I_1 \cdots \forall I_n F(I_1, \dots, I_n)$, where F is a formula without any quantification over ideals, then $G \in \text{Th}_1(\mathbf{BA}^\omega)$ iff $F(I_1, \dots, I_n)$ is true in every countable Boolean algebra $\mathfrak{B} = \langle B, U, \cap, ', I_1, I_2, \dots \rangle$, where $I_1, I_2, \dots$, are ideals of B . Using the Skolem–Löwenheim theorem we immediately get:

THEOREM 17 (RABIN [1969]). *The elementary theory of all Boolean algebras with a sequence of distinguished ideals is decidable.*

This theorem considerably strengthens the result of ERSHOV [1964] which asserts the decidability of Boolean algebras with a distinguished prime ideal (ultra-filter).

3.8. Non-classical logics

Thus far all the results presented in this paper dealt with theories formalized within classical logic. Many extensions and modifications of classical logic appear in the literature. These may take the form of rejection of certain axioms of classical logic, the intuitionistic logic is an example, or the addition of logical operators or connectives, as is being done in modal or tense logics. Important philosophical considerations and attitudes towards the foundations of mathematics and logic motivate the introduction and study of these systems.

While the decidability of the classical propositional calculus is trivial, the decidability of these fragments or enrichments (by addition of logical operators) of even the propositional logic is in most cases far from obvious. The method of interpretations turned out to be a powerful tool for settling almost all the decidability questions in this field. We shall illustrate this by two examples. The interested reader should consult the article of GABBAY [1975], which is the source for these examples, and where many other results and references are to be found.

The class of *modal propositional logics* to be considered here has, besides the usual propositional connectives, the operator $\Box$ which is intended to express *necessity*, so that $\Box A$ should be construed to mean: necessarily A .

A basic axiom system $C-2$, has all the theorems and rules of classical logic, and in addition the axioms and rules of inference

$$\Box[A \rightarrow B] \rightarrow [\Box A \rightarrow \Box B],$$

from $\vdash A \rightarrow B$ to infer $\vdash \Box A \rightarrow \Box B$.

The system K is obtained from $C-2$ by adding the rule

from $\vdash A$ to infer $\vdash \Box A$.

The system T is K plus the axioms $\Box A \rightarrow A$. And the system $S4$ is T plus the axioms $\Box A \rightarrow \Box \Box A$.

There are many other extensions of $C-2$. The particular axioms are chosen by the various authors on the basis of their beliefs as to what the correct properties of $\Box$ should be.

Let us now describe the intuitionistic *tense* logic J_t . This system will have, besides the connectives $\rightarrow, \vee, \wedge, \mathbf{f}$ (denoting falsehood), the operators G and H . For a formula A , GA reads: " A will always be true", and HA reads: " A was always true". The formula $\neg A$ abbreviates $A \rightarrow \mathbf{f}$.

The axioms and rules of inference for J_t will be those for the intuitionistic propositional logic (including modus ponens), and in addition

$$G[A \rightarrow B] \rightarrow [GA \rightarrow GB],$$

$$H[A \rightarrow B] \rightarrow [HA \rightarrow HB],$$

$$A \vee G \neg HA, \quad A \vee H \neg GA,$$

from $\vdash A$ to infer $\vdash GA$ and $\vdash HA$.

Kripke, Gabbay, and others, gave for many non-classical logics systems of semantics based on trees and valuations on trees. A formula would then be provable if it has a certain property under all possible valuations or interpretations. The detailed definition of interpretations would, of course, depend on the system of axioms in question.

It turns out that these tree-semantics are expressible in S2S and variants thereof. This makes it possible to derive a multitude of positive decidability results from the Tree Theorem.

4. Complexity of decision procedures

4.1. Turing machine computations

As remarked in the introduction, many results concerning lower bounds on the complexity of *solvable* decision problems appeared in recent years.

In particular almost all the theories discussed in this chapter were shown to have decision problems which do not admit of any simple decision procedure.

Since our aim will be to show that *every* decision procedure for a theory T is complex, we must settle on a definite formulation for algorithms and a definite convention for counting computational steps. We shall choose Turing-machine algorithms as our decision procedures, and the execution of an atomic instruction will count as a basic step.

The results will be of the form that for any decision procedure P for the theory T in question, there are sentences A of size n (i.e. written by use of n symbols) for which P will require at least $f(cn)$ steps to produce an answer as to whether $A \in T$ or not. The function $f(n)$ will be at least exponential 2^n , and c will be a fixed number $0 < c$. Because of the exponential nature of the results, it will make little difference which model of algorithms and computations is chosen. Computation-times in different models for the same algorithm differ by at most a polynomial transformation.

The method for obtaining these inherent complexity results rests on the following observation.

Let us transcribe programs for Turing machines in a uniform standard way by sequences $P \in \{0, 1\}^*$. For any word x define $l(x)$ to be the *length* of x , i.e. the number of symbols in x . In particular, for an integer written in binary notation, $l(n)$ is the number of digits in n .

Let T be a theory in the language L , and $f(k)$ be a function satisfying the following conditions. There exists a constant $0 < d$ so that for every program P and integer n , there exists a sentence $S(n, P)$ of L satisfying:

- (i) $l(S(n, P)) \leq d(l(n) + l(P))$,
- (ii) $S(n, P) \in T$ if and only if a computation by the program P on input n (viewed as a 0-1 sequence) halts in fewer than $f(l(n))$ steps.
- (iii) The formula $S(n, P)$ can be effectively computed from n, P in fewer than $g(l(n) + l(P))$ steps, where $g(k)$ is a fixed polynomial.

If $f(k)$ is a function growing at least at exponential rate, then under the above conditions there exists a constant $0 < c$ so that for infinitely many n there exists a sentence F of L , $l(F) = n$, for which P requires at least $f(cn)$ steps to decide whether $F \in T$.

The proof of the above statement is by a familiar diagonalization argument. One assumes, by way of contradiction, that there exists a decision procedure P for T which requires for every sentence F , fewer than $f(cl(F))$ steps to decide whether $F \in T$. If $c = 1/2d$ then, by use of the

sentence $S(n, P)$, one can construct a Turing machine which stops on an input n_0 if and only if it does not stop on that input.

4.2. The theory WS1S

MEYER [1975] has proved that the decision problem of WS1S is of a very high inherent complexity.

Define a function $F(n, m)$ by

$$F(n, 1) = 2^n, \quad F(n, m + 1) = 2^{F(n, m)}, \quad m = 1, 2, \dots$$

If $0 < d$, then $f(n) = F(n, [dn])$ is a function which is an exponentiation by a linear stack of 2 's.

THEOREM 18. *There exists a constant $0 < d$ so that for the function $f(n) = F(n, [dn])$, and every algorithm P for solving the decision problem of WS1S, there exist infinitely many formulas A so that P requires more than $f(l(A))$ steps to decide whether $A \in \text{WS1S}$.*

PROOF (outline). We have available in the language of WS1S variables $\alpha, \beta, \dots$, ranging over finite subsets of ω . A pair of subsets α, β can be used to code a sequence $p \in \{0, 1\}^*$, $l(p) = c(\alpha)$. If $\alpha = \{i_0 < i_1 < \dots < i_{k-1}\}$, then $i_j \in \beta$ if and only if $p(j) = 1$. For a fixed α and variable β , the pairs (α, β) will run through codes of all sequences p such that $l(p) = c(\alpha)$.

For the above α and $x \in \alpha$, $y \in \alpha$, we shall say that x and y are d apart in α if $x = i_j$, $y = i_{j+d}$, for some $j \leq k - 1 - d$.

One can now show that for every n there exist two formulas $A_n(\alpha)$ and $D_n(\alpha, x, y)$ of WS1S which are of length $O(n)$ and have the following properties. $A_n(\alpha)$ implies that α has a certain structure and is at least of cardinality $(F(n, n))^2$. For sets α for which $A_n(\alpha)$ holds, $D_n(\alpha, x, y)$ means that x and y are at distance $F(n, n)$ apart in α .

Suppose that we have a Turing machine computation with fewer than $F(n, n)$ steps. Then the machine-head will never be farther than $F(n, n)$ squares away from the starting square. We can assume without loss of generality that the machine never crosses to the left of the starting square.

We can string out in order, from left to right, the complete descriptions of the stretch of the first (leftmost) $F(n, n)$ squares after the execution of each of the machine-instructions. This will be a sequence of length at most $(F(n, n))^2$. This sequence can be coded by use of an $\alpha \subset \omega$ which satisfies $A_n(\alpha)$, and additional sets $\beta_0, \beta_1, \dots, \beta_k$. The pair (α, β_0) will code the tape-contents, and $((\alpha, \beta_1), \dots, (\alpha, \beta_k))$ will code the sequence of head locations and machine states.

The formula $D_n(\alpha, x, y)$ will serve as a “ruler” measuring off stretches of length $F(n, n)$. Together with the (definable) order on ω , it will enable us to express the fact that two consecutive stretches of the sequence coded by $(\alpha, \beta_0, \dots, \beta_k)$ are related by an execution of a single Turing machine instruction.

Filling out the details and combining the above ideas, it is possible to show that there exists for WS1S a construction of a formula $S(n, P)$ with the properties enumerated in 4.1. This entails Theorem 18 $\square$

It was independently observed by E. Robertson and by L. Stockmeyer (in his thesis) that a close examination of the full proof of Theorem 18 reveals that it will go through for sentences pertaining to $\langle \omega, \leq \rangle$ which are universal monadic second-order. This means sentences which may contain set quantifiers but these are all $\forall$ quantifiers and appear at the beginning of the sentence. In fact, a single set variable will suffice. A method of direct interpretations will yield from this more detailed result the following theorem due to MEYER [1974, 1975].

THEOREM 19. *The first-order theory $\text{Th}(\text{OR})$ of linearly ordered sets has inherent complexity $F(n, [dn])$ for some $0 < d$.*

The detailed formulation of Theorem 19, as well as of the results in the next subsection, is as in Theorem 18.

An analysis of the automata-theory based decision procedures for WS1S and even S2S shows that they run in time $F(n, [cn])$ for formulas A of size n , for an appropriate $0 < c$. In view of Theorems 18–19 these results are, qualitatively, best possible. There is, of course, the question of the height $[cn]$ of the stack of 2's, but this depends on the notation for the formulas and does not seem to be readily answerable.

4.3. Theories of addition and real-closed fields

For the classical theories $\text{Th}(\langle \omega, + \rangle) = \text{PAR}$, and the theory of the field of real numbers $\text{Th}(\text{RLC})$, the inherent complexity results are not as devastating as for WS1S. It does, however, turn out that these theories are at least exponentially complex, and in some cases super-exponentially complex. Thus the contention that the existence of a decision procedure trivializes these theories is not justified.

THEOREM 20 (FISCHER and RABIN [1974]). *There exists a constant $0 < c$ so*

that the decision problem of Presburger's arithmetic PAR is at least of complexity $2^{2^{cn}}$.

PROOF (outline). We saw that the ability to establish inherent complexity results for a complexity function $f(n)$, rests on the possibility to code within the theory by formulas of size $O(n)$ sequences of length $(f(n))^2$.

There exist in the language of $\langle \omega, + \rangle$ formulas $P_n(x, y, z)$ of size $O(n)$, which are true for any $x, y, z \in \omega$ if and only if $x, y, z < F(n, 3)$ and $x \cdot y = z$. Thus such a formula, which involves only $+$ and is of size $O(n)$, codes the multiplication table up to 2^{2^n} . Using integers to code 0-1 sequences, it is now possible to code sequences of length up to $(2^{2^n})^2$ by employing $P_{n+1}(x, y, z)$. $\square$

The lower bound for the complexity of $\text{Th}(\text{RLC}) = \text{Th}(\langle R, +, \cdot \rangle)$, where R is the field of real numbers, is obtained by considering just $\langle R, + \rangle$.

THEOREM 21 (FISCHER and RABIN [1974]). *$\text{Th}(\langle R, + \rangle)$, and consequently also $\text{Th}(\text{RLC})$, are of inherent complexity at least 2^{cn} for some $0 < c$.*

The proof is similar to the proof of Theorem 20. In this case it is possible to reproduce (up to isomorphism) by a short formula the multiplication table of integers up to 2^{2^n} .

For the theory of $\mathcal{M} = \langle \omega, \cdot \rangle$ of the integers under multiplication, the situation is even worse according to a theorem mentioned in FISCHER and RABIN [1974], the proof of which will be given in a forthcoming paper of Fischer and Rabin.

THEOREM 22. *The theory $\text{Th}(\omega, \cdot)$ of multiplication of natural numbers is of inherent complexity at least $F(cn, 3)$, i.e. $2^{2^{2^{cn}}}$, for some $0 < c$.*

Algorithms carefully constructed by various researchers strongly suggest that the above lower-bound results are best possible.

4.4. Propositional calculus and $P = NP$

It is customary in the study of abstract computation-models to make a distinction between deterministic and non-deterministic algorithms. When presented with a state-symbol combination, a Turing machine will execute a definite basic computational step (atomic move). The overall course of the computation is, therefore, completely determined by the Turing

machine (program), the starting state, and the initial tape-input. The deterministic mode is, of course, a feature of all present-day computers.

The notion of *non-deterministic* computations, or programs, is of fundamental importance in theoretical studies of the properties of algorithms. A non-deterministic program P allows, when presented with a state-symbol combination, the execution of one out of *possibly several* basic moves. For example state q_3 , when presented with 1, may call for either $(0, L, 7)$ (erase 1, move to left, go to state q_7) or $(1, R, 15)$. Thus, in a non-deterministic program, to each pair (q, b) where q is a state and b a symbol, there corresponds a set of triplets (c, M, q_i) , c is a symbol, $M \in \{L, R\}$, q_i is a state.

When started in state q_0 on an input tape, the program P may be able to go through any one of several sequences of basis steps, i.e. perform different computations on the input. It should be borne in mind that in each particular run a definite unique computation is performed. But several different runs, or *threads*, may be possible.

Let us illustrate the idea by showing that there is a non-deterministic program P which will factor any composite number n in $f(l(n))$ steps where $f(k)$ is a polynomial.

The program P has non-deterministic instructions enabling it, when given input n (in binary notation), to write on the tape any two numbers $1 < b, c < n$. As observed before, in any given run, one pair (b, c) will be written. But for every pair, there exists a run producing that pair. After b, c was produced, the program switches to a deterministic mode, calculates $b \cdot c$ and checks whether $n = b \cdot c$. The machine will stop only if the test showed equality.

We may observe the following features. Not every computation by P on n will halt. But if n is indeed composite then there are computations which will halt after a number of computational steps which is polynomial in the size $l(n)$ of the input.

This can be summarized by saying that compositeness of numbers can be non-deterministically recognized in polynomial time.

Consider now the problem of determining whether a propositional formula $F(p_1, \dots, p_n)$ has a truth-values substitution for the propositional variables, so that F becomes true. This is the *satisfiability* problem for the propositional calculus.

Since $F(p_1, \dots, p_n)$ is not satisfiable if and only if $F(p_1, \dots, p_n)$ is a formal theorem of propositional calculus, the satisfiability problem is closely related to the decision problem of PC.

It is again easy to construct a non-deterministic program which will

determine whether F is satisfiable by a number of steps which is polynomial in $l(F)$.

Does there exist an ordinary, deterministic, decision procedure for satisfiability which requires time (i.e. number of steps) which is just polynomial in the size of the formula? The polynomial in question may, of course, be faster growing than the polynomial for the non-deterministic program.

The answer to this question is not known. However COOK [1971] has shown that:

THEOREM 23. *If the satisfiability problem of the propositional calculus can be (deterministically) solved in polynomial time, then any problem which can be solved non-deterministically in polynomial time can also be solved in polynomial time by a deterministic algorithm.*

Thus the question whether there exists an efficient (polynomial) algorithm for satisfiability is equivalent to the question whether the class P of algorithms requiring polynomial time is equipotent with the class NP of non-deterministic algorithms requiring polynomial time. This is the celebrated $P = NP$ problem.

The algorithms in NP are very powerful. For example, an isomorphism between two given graphs of size n can be non-deterministically found in polynomial time. Similarly for an Hamiltonian circuit. These are difficult combinatorial-computational problems which defied repeated attempts at simple solutions.

Cook, KARP [1972], and others, found many examples of combinatorial decision problems which are reducible and in a certain sense equivalent to the satisfiability problem. The weight of this evidence may point in the direction that the satisfiability problem, being so powerful, is not of polynomial complexity and hence $P \neq NP$. But this fundamental question is, as yet, unanswered.

References

- AX, J.
 [1968] The elementary theory of finite fields, *Ann. of Math.*, **88**, 239–271.
 AX, J. and S. KOCHEN
 [1965a] Diophantine problems over local fields I, *Am. J. Math.* **87**, 605–630.
 [1965b] Diophantine problems over local fields II: A complete set of axioms for p -adic number theory, *Am. J. Math.*, **87**, 631–648.

- [1966] Diophantine problems over local fields III: Decidable fields, *Ann. of Math.*, **83**, 437–456.
- BÜCHI, J.R.
 [1960] Weak second order arithmetic and finite automata, *Z. Math. Logik Grundlagen Math.*, **6**, 66–92.
 [1962] On a decision method in restricted second order arithmetic, in: *Logic, Methodology and Philosophy of Science*, Proceedings of the 1960 Congress (Stanford Univ. Press, Stanford, CA) pp. 1–11.
- COHEN, P.J.
 [1969] Decision procedures for real and p -adic fields, *Comm. Pure Appl. Math.*, **22**, 131–151.
- COOK, S.A.
 [1971] The complexity of theorem proving procedures, Proceedings of the 3rd Annual ACM Symposium on theory of computing, pp. 151–158.
- EHRENFUCHT, A.
 [1959] Decidability of the theory of linear ordering relation, *Notices Am. Math. Soc.*, **6**, 268–269.
- ELGOT, C.C.
 [1961] Decision problems of finite automata design and related arithmetics, *Trans. Am. Math. Soc.*, **98**, 21–51.
- ERSHOV, YU. L.
 [1964] Decidability of relatively complemented distributive lattices and the theory of filters (in Russian), *Algebra i Logika* **3**, 17–38.
- FEFERMAN, S. and R.L. VAUGHT
 [1959] The first order properties of products of algebraic systems, *Fund. Math.*, **47**, 57–103.
- FISCHER, M.J. and M.O. RABIN
 [1974] Super exponential complexity of Presburger's arithmetic, *SIAM-AMS Proceedings* **7**, 27–41.
- GABBAY, D.M.
 [1975] Decidability results in non-classical logics, Part I, *Ann. Math. Logic*, **8**, 237–295.
- KARP, R.M.
 [1972] *Reducibility among Combinatorial Problems, Complexity of Computer Computations*, edited by R.E. Miller and J.W. Thatcher (Plenum Press, New York) pp. 85–104.
- LAUCHLI, H. and J. LEONARD
 [1966] On the elementary theory of linear order, *Fund. Math.*, **59**, 109–116.
- MEYER, A.R.
 [1975] The inherent complexity of theories of ordered sets, in: *Proceedings of the International Congress of Mathematics*, Vancouver 1974, Vol. 2, Canadian Mathematical Congress, pp. 477–482.
- MOSTOWSKI, A.
 [1952] On direct products of theories, *J. Symbolic Logic*, **17**, 1–31.
- PRESBURGER, M.
 [1929] Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, *Comptes Rendus du I^{er} Congrès des Mathématiciens des Pays Slaves*, Warszawa, pp. 92–101.
- RABIN, M.O.
 [1965] A simple method for undecidability proofs and some applications, in: *Logic, Methodology and Philosophy of Science II*, edited by Y. Bar-Hillel (North-Holland, Amsterdam) pp. 58–68.
 [1969] Decidability of second order theories and automata on infinite trees, *Trans. Am. Math. Soc.*, **141**, 1–35.

ROBINSON, A.

[1956] *Complete Theories* (North-Holland, Amsterdam).

SZMIELEW, W.

[1954] Elementary properties of Abelian groups, *Fund. Math.*, **41**, 203–271.

TARSKI, A.

[1949] Arithmetical classes and types of Boolean algebras (Preliminary report), *Bull. Am. Math. Soc.*, **55**, 64.

TARSKI, A.

[1951] *A Decision Method for Elementary Algebra and Geometry*, 2nd revised ed. (Berkeley and Los Angeles).

TARSKI, A. and A. MOSTOWSKI

[1949] Arithmetical classes and types of well ordered systems, *Bull. Am. Math. Soc.*, **55**, 65.

Degrees of Unsolvability: A Survey of Results*

STEPHEN G. SIMPSON

Contents

1. Introduction	632
2. Structure of the degrees without jump	635
3. The jump operator	639
4. $V = L$ versus PD	641
5. Between $\mathbf{0}$ and $\mathbf{0}'$	645
6. Degrees of complete theories	647
References	649

* During preparation of the first two drafts of this chapter, the author was supported by a grant from the Science Research Council of the United Kingdom. The author records here his gratitude to the Mathematical Institute and Wolfson College of the University of Oxford, for hospitality during the academic year 1974–1975. The preparation of the final draft was partially supported by NSF grant MSP 75–07408 at Penn State.

The author is grateful to Professors Barwise, Jockusch and Kreisel for helpful correspondence.

1. Introduction

This chapter is intended for readers who have at least a nodding acquaintance with some basic ideas from recursive function theory. The ideas can be found in Chapter C.1.

The structure of the degrees is essentially a classification of all sets of integers according to complexity. The recursive sets of integers comprise the lowest level of complexity. A *degree* (sometimes called a Turing degree or a degree of unsolvability) is just an equivalence class of sets of integers, under the following equivalence relation: S_1 is recursive relative to S_2 , and S_2 is recursive relative to S_1 . Trivially, each set of integers falls into one of these equivalence classes. The degrees are partially ordered as follows: $d_1 > d_2$ if and only if sets in the equivalence class d_1 are more nonrecursive than sets in the equivalence class d_2 .

The simple idea just described leads to a rich and interesting theory. In fact, for many years now, degree theory has been one of the most technical and highly developed parts of mathematical logic. There are literally hundreds of papers in the literature, all devoted exclusively to degrees. The standard of originality in these papers is very high. Although certain ideas recur, the variety of methods employed is enormous. Some workers even make a point of not publishing a theorem unless the proof illustrates a new technique.

The situation just described presents a hardship to him who attempts to bring order and clarity to degree theory. Nevertheless, there do exist some truly excellent surveys, including LACHLAN [1973], SACKS [1963], SHOENFIELD [1971], SOARE [1976], and YATES [1976]. (Perhaps SHOENFIELD [1971] is best for the beginner.) In keeping with the way degree theory has developed, all of the papers just mentioned lay heavy emphasis on *methods of proof*.

In the present survey we indulge in a few methodological remarks. However, we have made a conscious decision to neglect methodology and to concentrate instead on *results*. Thus we try to present those theorems whose statements alone shed the most light on the structure and uses of degrees. Such theorems do not always have the most interesting proofs. Our reasons for this choice of emphasis are the following:

(1) As mentioned above, there already exist several excellent methodological surveys, on which we could not possibly hope to improve.

(2) Our typical reader is probably not himself planning to perform research in degree theory. He is therefore likely to be more interested in results than in methods of proof.

(3) We feel that now would be a good time for degree theorists to take a critical, backward look at the concrete accomplishments in their field. We hope that a survey of results will promote this kind of introspection and thereby suggest directions for future research.

Another aspect of degree theory which we neglect here is *history*. This is partly because we prefer to discuss later, comprehensive results instead of earlier, fragmentary ones. Besides, an historical approach might be misleading, inasmuch as the general conception of what degree theory is all about seems to have changed over the years. Nevertheless, in order not to commit the crime of being totally ahistorical, we now point out the obvious fact that the published literature of degree theory begins with papers of Emil L. Post. (Sections 5 and 6 of the present survey discuss problems which have their origin in POST [1944]. Sections 2, 3, and 4 are closer in spirit to POST [1948] and KLEENE and POST [1954]. Serious historical difficulties arise from the fact that much of Post's work remains unedited, unpublished, and inaccessible.)

Since the days of Post, degree theory has turned out to have a number of connections with other parts of mathematical logic. Unfortunately, limitations of space prevent our discussing these aspects here. Another important topic which we omit is generalizations of degree theory. A recent survey of α -degrees is contained in Chapter C.5. A degree notion which is of particular importance for descriptive set theory is discussed in the forthcoming Ph.D. theses of J. Steel and W. Wadge, both of the University of California at Berkeley.

The rest of this introduction consists of a brief definition of some of the basic notions of degree theory. For more details, the reader may consult Section 8 of Chapter C.1.

We use ω to denote both the smallest infinite ordinal and the set $\{0, 1, 2, \dots\}$ of nonnegative integers. We use 2^ω to denote the set of all $\{0, 1\}$ valued functions on ω . We use letters such as f, g, h to denote elements of 2^ω .

For $f, g \in 2^\omega$ we use $f \oplus g$ to denote the unique function $h \in 2^\omega$ such that $h(2n) = f(n)$, $h(2n+1) = g(n)$ for all $n \in \omega$. We write $f \leq_T g$ (read: f is recursive in g , f is Turing reducible to g , f is computable from g) if there exists an algorithm which computes $f(n)$ from n using an oracle for g , for all $n \in \omega$. We assume a fixed Gödel numbering of the algorithms. For all $f \in 2^\omega$ we define $f^* \in 2^\omega$ by: $f^*(n) = 1$ if the n -th algorithm eventually halts if started with input n and oracle f ; $f^*(n) = 0$ otherwise.

1.1. PROPOSITION. (i) $f \leq_T f$.

(ii) $f \leq_T g, g \leq_T h$ implies $f \leq_T h$.

(iii) $f \oplus g \leq_T h$ if and only if $f \leq_T h, g \leq_T h$.

(iv) $f \leq_T f^*$ and not $f^* \leq_T f$.

(v) $f \leq_T g$ implies $f^* \leq_T g^*$.

Two functions $f, g \in 2^\omega$ are said to have the same *degree* if $f \leq_T g$ and $g \leq_T f$. The set of all degrees is denoted D . Boldface letters such as $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}$ are used to denote degrees. The degree of f is denoted $\deg(f)$. The degree of a set $A \subseteq \omega$ is the degree of its characteristic function $c_A \in 2^\omega$.

Let $\mathbf{a} = \deg(f), \mathbf{b} = \deg(g)$. A binary relation $\leq$ on D is defined by $\mathbf{a} \leq \mathbf{b}$ if and only if $f \leq_T g$. A binary operation $\cup$ on D is defined by $\mathbf{a} \cup \mathbf{b} = \deg(f \oplus g)$. By 1.2 (ii) and 1.2(v), D is an upper semilattice under $\cup$. A unary operation $j : D \rightarrow D$, called the *jump operator*, is defined by $j(\mathbf{a}) = \mathbf{a}' = \deg(f^*)$. A distinguished element of D is defined by $\mathbf{0} = \deg(\lambda n \cdot 0)$. Thus $\mathbf{0}$ is the degree of recursive functions.

1.2. PROPOSITION. (i) D has cardinality $2^{\aleph_0}$.

(ii) D is partially ordered by $\leq$.

(iii) A subset of D has an upper bound (under $\leq$) if and only if it is countable.

(iv) $\mathbf{0}$ is the least element of D .

(v) $\mathbf{a} \cup \mathbf{b}$ is the least upper bound of $\mathbf{a}, \mathbf{b}$.

(vi) $\mathbf{a} < \mathbf{a}'$ for all $\mathbf{a}$.

(vii) $\mathbf{a} \leq \mathbf{b}$ implies $\mathbf{a}' \leq \mathbf{b}'$.

The jump operator will play a fundamental role in this chapter. We therefore mention two important characterizations of it:

(1) A subset of ω is said to be *recursively enumerable in a degree $\mathbf{a}$* if it is either empty or the range of a function $p : \omega \rightarrow \omega$ which is recursive in $\mathbf{a}$. A degree $\mathbf{b}$ is said to be *r.e. in $\mathbf{a}$* if $\mathbf{b}$ is the degree of a set which is recursively enumerable in $\mathbf{a}$. Then: $\mathbf{a}'$ is the largest degree which is r.e. in $\mathbf{a}$.

(2) We say that f is *limit recursive in g* if there exists a function $p : \omega \times \omega \rightarrow \omega$ such that p is recursive in g and $f(m) = \lim_n p(m, n)$ for all $m \in \omega$. Then for $\mathbf{a} = \deg(f), \mathbf{b} = \deg(g)$, we have: $\mathbf{a} \leq \mathbf{b}'$ if and only if f is limit recursive in g .

If $\mathbf{a} = \deg(f)$ and $n \in \omega$, we write $\mathbf{a}^{(n)} = \deg(f^{(n)})$ where $f^{(0)} = f, f^{(n+1)} = (f^{(n)})^*$. Thus $\mathbf{a}^{(0)} = \mathbf{a}$ and $\mathbf{a}^{(n+1)} = (\mathbf{a}^{(n)})'$ so in effect we have defined *finite iterates of the jump operator*. The beginning of an extension into the

transfinite is obtained by putting $a^{(\omega)} = \deg(f^{(\omega)})$ where $f^{(\omega)} \in 2^\omega$ is defined by

$$f^{(\omega)}(2^m \cdot (2n + 1) - 1) = f^{(m)}(n)$$

for all $m, n \in \omega$. Note that the degree $a^{(\omega)}$ is an upper bound of the increasing sequence $a, a', a'', \dots, a^{(n)}, a^{(n+1)}, \dots$ ($n \in \omega$). Further transfinite iterates of the jump operator will be defined in Section 4.

2. Structure of the degrees without jump

In this section we discuss the structure of D , the set of all degrees, regarded as either a partially ordered set $\langle D, \leq \rangle$ or an upper semilattice $\langle D, \cup \rangle$. Results whose statements mention the jump operator are reserved for later sections. The trend of the results in this section is that the structure of D is very rich, indeed sometimes intractable, but has a number of pleasing properties such as 2.2 and 2.3.

We begin by discussing the types of suborderings of D . Let S be a partially ordered set which is embeddable in D . Then trivially, by 1.2, we have:

- (i) the cardinality of S is $\leq 2^{\aleph_0}$;
- (ii) every element of S has at most countably many predecessors. A problem of SACKS [1963] which remains open is whether the converse is true, i.e. whether every partially ordered set satisfying (i) and (ii) is embeddable in D . The main positive result on this problem is the following, which incidentally solves the problem completely if the continuum hypothesis holds.

2.1 THEOREM (SACKS [1963]). *Let S be a partially ordered set which satisfies conditions (i), (ii) and (iii): every element of S has at most $\aleph_1$ successors. Then S is order-embeddable in D .*

Of course a corollary of 2.1 is that every countable partially ordered set is embeddable in D .

In the proof of 2.1, an embedding of S into D is obtained as the limit of a transfinite sequence of extensions to successively larger subsets of S . This suggests a difficult general problem: when can an embedding of a partially ordered set into D be extended to an embedding of a larger, partially ordered set into D ? An interesting special case of this problem involves *independent sets*, i.e. sets of nonzero degrees such that no element of the set

is less than or equal to the least upper bound of finitely many other elements of the set. By Zorn's Lemma, any independent set can be extended to a maximal independent set. It is not hard to show that there exists an independent set of cardinality $2^{\aleph_0}$, and that every maximal independent set has cardinality $\geq \aleph_1$ (more generally $\geq \aleph_{\alpha+1}$ assuming Martin's axiom for $\aleph_\alpha$). SACKS [1963] asks: does every maximal independent set have cardinality $2^{\aleph_0}$? The answer to this question may well be independent of ZFC.

We now introduce the important topic of ideals in D . A set $I \subseteq D$ is called an *ideal* if

- (i) $0 \in I$;
- (ii) $a \leq b \in I$ implies $a \in I$;
- (iii) $a, b \in I$ implies $a \cup b \in I$.

For example, if a is any degree then we have the *principal ideal*

$$I(a) = \{d \mid d \leq a\}.$$

Note that any principal ideal is countable. A nonprincipal, countable ideal is generated by any countable ascending sequence of degrees, e.g. $\{0^{(n)} \mid n \in \omega\}$. Another example of a nonprincipal ideal is D itself.

Our use of the word ideal is not standard terminology, but it is certainly natural, since conditions (i)–(iii) are equivalent to saying that I is the kernel of a homomorphism of $\langle D, \cup, 0 \rangle$ onto another upper semilattice with distinguished least element. Later we shall have more to say about the images of these homomorphisms.

For the moment we regard an ideal as simply a subordering of D and ask: what can we say about its order type? Clearly an ideal is an upper semilattice with a least element, but can we say more? The answer in the countable case is very pleasing:

2.2. THEOREM (LACHLAN and LEBEUF [1976]). *Every countable upper semilattice with a least element is isomorphic to a countable ideal in D .*

An important special case of 2.2, due to SPECTOR [1956], is that there exists a *minimal* degree, i.e. a degree m such that 0 is the unique degree less than m .

The proof of 2.2 is combinatorially intricate. However, the basic recursion-theoretic idea of the proof goes back to SPECTOR [1956] and is not difficult. The history of 2.2 and a major contribution to the combinatorial part of its proof are in LERMAN [1971].

Uncountable generalizations of 2.2 are largely mysterious; e.g., it is open

whether D has an ideal of order type $\aleph_1$. YATES [1970] remarks that this latter statement is consistent¹ with ZFC, and makes conjectures. One isolated fact is that D has an ideal which is order-isomorphic to the lattice of finite sets of real numbers (cf. THOMASON [1970]). An easy corollary of this fact is that every maximal, pairwise incomparable set of degrees has cardinality $2^{\aleph_0}$ (SACKS [1963]).

The next theorem says something important about the way a countable ideal sits in D .

2.3. THEOREM (SPECTOR [1956]). *Let I be any countable ideal in D . Then there exists a (nonunique) pair of degrees a_1, a_2 such that*

$$I = \{d \mid d < a_1 \text{ and } d < a_2\}.$$

In the special case of principal ideals, 2.3 tells us that every degree is the greatest lower bound of two larger degrees. A corollary of 2.3 for nonprincipal ideals is that an infinite ascending sequence of degrees can never have a least upper bound.

In general, a pair a_1, a_2 satisfying the conclusion of 2.3 is called an *exact pair* for I . The existence of exact pairs implies that in the first-order theory of $\langle D, \cup \rangle$ we can talk about and quantify over arbitrary countable ideals. This expressive power is exploited in the proof of Theorem 2.7 below. Further exploitation of exact pairs occurs in Theorem 4.3.

We now consider what happens to D when we “mod out” by a countable ideal I . Intuitively, the idea is to pretend that all functions in

$$M_I = \{f \mid \deg(f) \in I\}$$

are recursive, and ask what effect this identification has on the structure of D . There are two distinct ways to make this idea precise:

(1) Define an equivalence relation $\equiv_I$ on D by: $a \equiv_I b$ if and only if $a \cup d = b \cup d$ for some $d \in I$. Let D/I be the set of all equivalence classes.

(2) Let $D_I = \{a \mid a > d \text{ for all } d \in I\}$.

Both D/I and D_I are upper semilattices. D/I is algebraically more natural since it has a least element, viz. I itself. D/I is in fact just the quotient of D by I in the category of upper semilattices with distinguished least element. By 2.3 D_I can never have a least element. (However, there is a natural isomorphism of D_I onto a certain upward closed subset of D/I . If I is principal, then this subset consists of the nonzero elements of D/I .)

¹ The metalanguage for this paper is ZFC, Zermelo–Fraenkel set theory with the axiom of choice. When discussing questions of consistency and independence, we tacitly assume that ZFC is consistent.

An interesting, general phenomenon is that many structural results about D hold also for D/I and D_I when I is a countable ideal, with only slight changes in the proofs. For instance, 2.1 is true verbatim with D replaced by D/I or D_I , I countable. The routine procedure, whereby theorems and their proofs are generalized from D to D/I or D_I , is called *relativization* to I (cf. Section 9.3 of ROGERS [1967a]). The validity of this procedure rests on the fact that M_I has many of the same closure properties as the set of recursive functions; all the more so when I is principal. Usually one speaks of relativization to a degree a rather than to the principal ideal $I(a)$. The relativized versions of many theorems such as 2.2 have been verified for principal ideals (but sometimes not for arbitrary countable ideals, except in special cases).

A tantalizing conjecture of ROGERS [1967a], p. 261) is that for all principal ideals $I(a)$, $D/I(a)$ is isomorphic to D . Certainly $D/I(a)$ and D share many structural properties. It is also natural to consider the following generalization of Rogers' conjecture: for all countable ideals I ,

$$D_I \cong D/I - \{I\} \cong D - \{0\}.$$

Two further open problems, also due to ROGERS [1967b], are whether any, or every, nonzero degree is invariant under all automorphisms of $\langle D, \cup \rangle$. All of these Rogers problems are wide open. (If we change the problems by requiring isomorphisms and automorphisms to be jump-preserving, then considerable progress has been made. See Corollaries 3.6 and 3.8 below.)

So far in this section we have safely ignored the jump operator. We now wish to point out that there are many theorems, about the upper semilattice structure of D , which do not mention jump but whose proofs use it. Perhaps the simplest example of such a theorem is the following. Say that a degree b *splits* if it is the least upper bound of two smaller degrees b_1 and b_2 . Not every nonzero degree splits, e.g. a minimal degree. However:

2.4. THEOREM. $\exists a \forall b (b > a \rightarrow b \text{ splits}).$

This is proved as follows. Take $a = 0'$. Given $b > 0'$, use Friedberg's jump-inversion theorem 3.1 to find a degree c such that $c' = c \cup 0' = b$. Then put $b_1 = c$, $b_2 = 0'$.

The next two theorems strengthen 2.4 and, like 2.4, are derived from theorems about the jump operator. Say that b is *cuppable* if for all nonzero $b_1 < b$ there exists $b_2 < b$ such that $b_1 \cup b_2 = b$.

2.5. THEOREM. $\exists a \forall b (b > a \rightarrow b \text{ is cuppable}).$

2.6. THEOREM. $\exists a \forall b (b > a \rightarrow b \text{ is the least upper bound of two minimal degrees})$.

For 2.5 we take $a = 0'$ and use 3.2 and a relativized version of Robinson's theorem 5.3. For 2.6 we take $a = 0''$ (cf. Theorem 2.4 of MARTIN and MILLER [1968]).

We end this section by giving a complete answer to a question which seems to have first been raised by Shoenfield (cf. SHOENFIELD [1965]). The question is: how complicated is the first-order theory of the upper semilattice $\langle D, \cup \rangle$?

2.7. THEOREM (SIMPSON [1977]). *The first-order theory of $\langle D, \cup \rangle$ is recursively isomorphic to the truth set of second-order arithmetic.*

Here is a sketch of the proof. By 3.4 we have the same result for the expanded structure $\langle D, \cup, j \rangle$ where j is the jump operator. In the proof of 3.4, the jump operator is used only to show that there exist certain configurations of degrees which encode second-order arithmetic. By using 2.3 we can speak about these configurations in the first-order theory of $\langle D, \cup \rangle$.

3. The jump operator

In the previous section, the jump operator $j : D \rightarrow D$ occurred as an auxiliary notion, used only in order to prove theorems which did not mention it. We now study the jump operator for its own sake. The basic result here is Friedberg's inversion theorem:

3.1. THEOREM (FRIEDBERG [1957b]). *For every degree $b \geq 0'$ there exists a such that $a' = a \cup 0' = b$.*

An easy corollary of 3.1 and 1.2 is that the range of the jump operator is precisely the set of degrees $\geq 0'$.

There is an extensive literature on the jump operator. Much of this literature concerns refinements of 3.1 in various directions. For instance, a simple modification of the proof of 3.1 yields the following useful result (see also SPECTOR [1956]):

3.2. THEOREM. *For any $b \geq 0'$ there exists an infinite set $\{a_i \mid i \in \omega\}$ such that $a_i \cap a_j = 0$ for all $i \neq j$, and $a'_i = a_i \cup 0' = b$ for all i .*

Other refinements of 3.1 involve restricting the domain of the jump operator. Thus, in Section 6 of SACKS [1963], it is shown that

$$\begin{aligned} \{a' \mid 0 < a < 0' \text{ and } a \text{ is r.e.}\} = \\ = \{b \mid b \geq 0' \text{ and } b \text{ is r.e. in } 0'\}. \end{aligned}$$

This beautiful result is also important historically because its proof contained the first major application of the so-called "infinite injury" priority method. Yet another striking refinement of 3.1, whose proof incidentally also requires a kind of infinite injury argument, is the following:

3.3. THEOREM (COOPER [1973]). *For any $b \geq 0'$ there exists a minimal degree m such that $m' = m \cup 0' = b$.*

We now discuss some recent results concerning first-order definability and automorphisms of the structure

$$\mathcal{D} = \langle D, \cup, j \rangle.$$

By *second-order arithmetic* we mean the first-order theory of the two-sorted structure

$$\mathcal{S} = \langle 2^\omega, \omega, +, \cdot, E \rangle$$

where $+$ and $\cdot$ are the usual arithmetical operations on ω , and $E : 2^\omega \times \omega \rightarrow \omega$ is defined by $E(f, n) = f(n)$. Good introductions to the recursion theoretic literature on second-order arithmetic are Section 16.2 of ROGERS [1967a] and Section 8.5 of SHOENFIELD [1967]. We are going to discuss a certain translation of the language of second-order arithmetic into the language of $\mathcal{D}$. To this end we need a special mapping $\Gamma : D \rightarrow 2^\omega$ defined by

$$\Gamma(d)(n) = \begin{cases} 1 & \text{if } 0^{(n+1)} \leq d \cup 0^{(n)}, \\ 0 & \text{otherwise.} \end{cases}$$

3.4. THEOREM (SIMPSON [1977]). *Let $\varphi(f_1, \dots, f_i, n_1, \dots, n_j)$ be a formula of second-order arithmetic. Then we can effectively find a formula $\varphi^*(x_1, \dots, x_i, y_1, \dots, y_j)$ of degree theory, such that for all $d_1, \dots, d_i \in D$ and $n_1, \dots, n_j \in \omega$,*

$$\mathcal{S} \models \varphi[\Gamma(d_1), \dots, \Gamma(d_i), n_1, \dots, n_j]$$

if and only if

$$\mathcal{D} \models \varphi^*[d_1, \dots, d_i, 0^{(n_1)}, \dots, 0^{(n_j)}].$$

PROOF (sketch). Formulas of first-order arithmetic are handled by showing that the set $\Omega = \{0^{(n)} \mid n \in \omega\}$ and the relations $\{\langle 0^{(m)}, 0^{(n)}, 0^{(p)} \rangle \mid m + n = p\}$ and $\{\langle 0^{(m)}, 0^{(n)}, 0^{(p)} \rangle \mid m \cdot n = p\}$ of “addition” and “multiplication” on Ω , are first-order definable in $\mathcal{D}$. Function quantifiers are handled by showing that Γ maps D onto 2^ω . $\square$

In order to draw some corollaries about automorphisms and definability in $\mathcal{D}$, we need the following rather easy proposition. Recall that the degree $0^{(\omega)}$ is a canonical upper bound to $\{0^{(n)} \mid n \in \omega\}$.

3.5. PROPOSITION (SIMPSON [1977]). *The relation $\{\langle a, b \rangle \mid 0^{(\omega)} \leq b = \deg(\Gamma(a))\}$ is first-order definable in $\mathcal{D}$.*

3.6. COROLLARY (Solovay). *Every degree $\geq 0^{(\omega)}$ is fixed by all automorphisms of $\mathcal{D}$.*

3.7. COROLLARY (SIMPSON [1977]). *An n -ary relation $R \subseteq \{d \mid 0^{(\omega)} \leq d\}^n$ is definable in $\mathcal{D}$ if and only if*

$$R^* = \{\langle f_1, \dots, f_n \rangle \mid R(\deg(f_1), \dots, \deg(f_n))\}$$

is definable in second-order arithmetic.

3.8. COROLLARY (SIMPSON [1977]). *The substructure of $\mathcal{D}$ whose universe is $\{d \mid 0^{(\omega)} \leq d\}$ is not elementarily equivalent to $\mathcal{D}$.*

Corollaries 3.6, 3.7 and 3.8 are fairly immediate consequences of 3.4 and 3.5. A different proof of 3.6 was discovered earlier by R.M. Solovay using observations in Section 5 of YATES [1972]. Jockusch has noted that these same observations show that in 3.6, $0^{(\omega)}$ can be improved to $0^{(6)}$. It remains open whether $\mathcal{D}$ has any automorphisms other than the identity.

4. V = L versus PD

In this section we discuss some aspects of the correlation between degree theory and axiomatic set theory. We begin with some historical remarks.

In the earliest days of forcing, many degree theorists noticed the strong resemblance between Cohen’s method and the well-developed technique of finite approximation in degree theory. Somewhat later, Sacks used analogies with degree theory to suggest new results and problems in

axiomatic set theory ("degrees of nonconstructibility", SACKS [1971]). However, direct connections between degrees and axiomatic set theory have come to light only very recently. To my knowledge, the literature prior to 1968 contains no hint of direct connections (although SACKS [1963] mentions some applications of measure theory and descriptive set theory).

The earliest papers in which concepts of axiomatic set theory are applied directly to degrees are BOLOS and PUTNAM [1968] and MARTIN [1968]. Subsequently, the correlation was found to be unexpectedly close and detailed. For instance, it follows from 3.7 that there is a first-order formula $\psi(x)$ of degree theory, such that for all degrees $\mathbf{d}$, $\mathcal{D} \models \psi[\mathbf{d}]$ if and only if $\mathbf{d}$ is constructible in the sense of GÖDEL [1939].

In our opinion, axiomatic set theory offers one of the most interesting problem areas for future research on degrees. (In fairness we point out that many of our fellow degree-theorists do not share this opinion.) We wish to present here some of the known results showing that various set theoretical hypotheses, such as $V = L$ (the "axiom" of constructibility) or PD (the "axiom" of projective determinacy), have striking consequences for the structure of the degrees.

A set of degrees $X \subseteq D$ is said to be *determined* if there exists a degree $\mathbf{a}$ such that either $\{\mathbf{d} \mid \mathbf{d} \geq \mathbf{a}\} \subseteq X$ or $\{\mathbf{d} \mid \mathbf{d} \geq \mathbf{a}\} \cap X = \emptyset$. Not every set of degrees is determined. However, there are many nontrivial theorems in the literature, each saying that some specific set of degrees is determined, one way or the other. For example, each of 2.4, 2.5, 2.6, 3.1 and 3.3 expresses an instance of determinacy.

Not only are many familiar subsets of D known to be determined, but the reader (even the expert degree theorist) will probably be unable to define in ZFC a set of degrees such that he can prove in ZFC that the set is *not* determined. These empirical phenomena lead to the formulation of the following heuristic principle:

4.1. HEURISTIC PRINCIPLE. *Let X be a "simple-minded" subset of D . Then X is determined.*

There is a close connection between determinacy and Gale–Stewart games. For general information about such games, the reader may consult Chapter C.8. The specific connection is as follows. Let X be a subset of D . Let two players, I and II, play an infinite game with perfect information, leading to the definition of a function $f \in 2^\omega$. The rules of this game are that I picks $f(0)$, then II picks $f(1)$, ..., then I picks $f(2n)$, then II picks $f(2n+1)$, ... Finally I wins if $\deg(f) \in X$, II wins otherwise. It can be

shown that X is determined if and only if one of the players has a winning strategy. (Furthermore, the degree a mentioned in the definition of determinacy can be taken to be the degree of a winning strategy.) This remark is due to MARTIN [1968].

Many true instances of Principle 4.1 can be verified by using the remark of the previous paragraph, plus recent results on Gale–Stewart games. For $X \subseteq D$ let us write $X^* = \{f \mid \deg(f) \in X\}$. Then we have:

4.2. THEOREM (MARTIN [1975, 1970, 1968]). *A set $X \subseteq D$ is determined under any of the following circumstances:*

- (i) X^* is Borel (i.e. Δ_1^1).
- (ii) X^* is analytic (i.e. Σ_1^1) and a Ramsey cardinal exists.
- (iii) X^* is projective (i.e. Σ_n^1 for some $n \in \omega$) and PD holds.

From axiomatic set theory, we know that it is impossible to prove the consistency with ZFC of the existence of a Ramsey cardinal or of PD. However, the inconsistency with ZFC of these hypotheses has not been proved.

In order to draw out an interesting consequence of 4.2(i), let $\{\varphi_n\}_{n \in \omega}$ be an enumeration of the sentences of the first-order language of upper semilattices. Since each principal ideal $I(\mathbf{b}) = \{\mathbf{d} \mid \mathbf{d} \leq \mathbf{b}\}$ is an upper semilattice, we may define the sets $X_n = \{\mathbf{b} \in D \mid I(\mathbf{b}) \models \varphi_n\}$. By 4.2(i), X_n is determined. Let

$$\psi_n = \begin{cases} \varphi_n & \text{if } \exists \mathbf{a} \{\mathbf{b} \mid \mathbf{b} \geq \mathbf{a}\} \subseteq X_n; \\ \neg \varphi_n & \text{if } \exists \mathbf{a} \{\mathbf{b} \mid \mathbf{b} \geq \mathbf{a}\} \cap X_n = \emptyset. \end{cases}$$

Then $\{\psi_n\}_{n \in \omega}$ is the theory of a “typical” principal ideal. I.e., there exists a degree $\mathbf{a}$ such that $I(\mathbf{b}) \models \psi_n$ for all $\mathbf{b} \geq \mathbf{a}$, $n \in \omega$.

Let us say that a set $X \subseteq D$ is (weakly) *definable* if it is first-order definable in the structure $\mathcal{D} = \langle D, \cup, j \rangle$ (allowing parameters from D). By 4.1 it is natural to ask whether every weakly definable set is determined. If PD holds, then this is the case by 4.2(iii). (In fact, 3.7 plus a recent result of Harrington make it appear probable that PD is *equivalent* to the assertion that every weakly definable subset of D is determined.) However, the negative answer is known to hold in a wide class of models of ZFC. Specifically, let $Y = \{\mathbf{d} \in D \mid \text{the hyperdegree of } \mathbf{d} \text{ is a minimal cover}\}$. Then by 3.7 or JOCKUSCH and SIMPSON [1976] Y is definable, but by SIMPSON [1975] Y is not determined if $V = L$ or a generic extension of L .

We have just pointed out that some pleasing results about $\mathcal{D}$ are gotten by assuming PD. We now wish to point out that the picture of $\mathcal{D}$ which we get by making the diametrically opposite assumption, $V = L$, is also very pretty.

Without any special assumptions, it can be shown that there exists a transfinite increasing sequence of degrees $0^{(\alpha)}$, $\alpha < \aleph_1^L$. (See also BOLOS and PUTNAM [1968] and JENSEN [1972].) The degrees in this sequence are naturally identified as *transfinite iterates of the jump operator*, i.e. we have:

- (i) $0^{(0)} = 0$;
- (ii) $0^{(\alpha+1)} = \text{jump}(0^{(\alpha)})$ for all α ;
- (iii) $0^{(\alpha)} < 0^{(\beta)}$ for $\alpha < \beta$;
- (iv) for each limit ordinal $\lambda < \aleph_1^L$, $0^{(\lambda)}$ is the “least natural” upper bound for $\{0^{(\alpha)} \mid \alpha < \lambda\}$ in D .

Moreover, if $V = L$, then the degrees $0^{(\alpha)}$, $\alpha < \aleph_1^L$ are exhaustive in the sense that the ideal which they generate is all of D . In particular, these degrees form a natural example of an undetermined set.

In order to explain clause (iv) above, recall that by 2.3 the degrees $0^{(\alpha)}$, $\alpha < \lambda$, can never have a *least* upper bound. What (iv) says is that $0^{(\lambda)}$ is a particular upper bound which arises naturally in terms of the algebraic structure of $\mathcal{D} = \langle D, \cup, j \rangle$. Let us write I_λ for the countable ideal generated by $\{0^{(\alpha)} \mid \alpha < \lambda\}$. We now describe (in a special case) the exact nature of the degree theoretic dependence of $0^{(\lambda)}$ on I_λ . (See also BOYD, HENSEL and PUTNAM [1969] and JOCKUSCH and SIMPSON [1976].) If I is any countable ideal in D , a degree d is said to be *n-exact over I* (where n is a positive integer) if d is the unique least degree of the form $(a \cup b)^{(n)}$ where a, b is an exact pair for I . Let β_0 be the ordinal of ramified analysis, which can also be defined as the least ordinal β such that L_β is a model of ZFC minus the power set axiom. It is well known that β_0 is a rather large, but countable, ordinal number.

4.3. THEOREM. *For any limit ordinal $\lambda < \beta_0$ we can find a least positive integer $n = n_\lambda$ such that there exists a degree which is n -exact over I_λ . Moreover $0^{(\lambda)}$ is this unique degree.*

As λ ranges over the limit ordinals less than β_0 , it can be shown that n_λ ranges over all the integers $n \geq 2$. Furthermore, if λ is β_0 itself, then n_λ is undefined. It is possible to extend 4.3 beyond β_0 by considering a notion of ν -exactness where ν is an ordinal. In order to continue beyond $\aleph_1^L$, it is necessary to supplement Jensen’s “fine structure of L ” (JENSEN [1972]) with Solovay’s “fine structure of $L(\mu)$ ” (unpublished).

5. Between 0 and 0'

The results which were mentioned in previous sections belong to what might be called "global degree theory", i.e. they deal with general, structural properties of $\langle D, \cup \rangle$ and $\langle D, \cup, j \rangle$. We now turn to "local degree theory", i.e. the theory of the degrees $\leq 0'$.

A subset of ω is said to be *recursively enumerable* if it is empty or the range of a recursive function from ω into ω . A degree is said to be *r.e.* if it is the degree of a recursively enumerable subset of ω . It is easy to see that 0 and 0' are r.e. degrees, and that every r.e. degree is $\leq 0'$. R.e. degrees were introduced by POST [1944] who posed the following famous problem: prove that there exists an r.e. degree between 0 and 0'. Post himself made some progress, but the problem remained unsolved until FRIEDBERG [1957a] and MUCHNIK [1956]. Ideas flowing from Post's problem and its solution have played a dominant role in local degree theory up to the present day.

The methods of proof in local degree theory are very sophisticated. For each of the theorems mentioned in this section, the general pattern of proof is as follows. A recursive construction in infinitely many stages is performed. There are infinitely many requirements to be satisfied. From time to time in the course of the construction, some of these requirements are seen to come into conflict with one another. The conflicts are resolved when they arise, according to a recursive scheme of priorities. Since requirements can be injured at various stages, a delicate argument is needed to show that each requirement is finally met.

A proof in the pattern just described is called a *priority argument*. The first such argument was used in the Friedberg-Muchnik solution of Post's problem. Extensions of the Friedberg-Muchnik method were developed for other problems by later workers, among them LACHLAN, SACKS, and YATES. In keeping with our general policy of concentrating on results rather than methods, we shall say no more about priority arguments here. The interested reader may consult the expository masterpieces of LACHLAN [1973], SHOENFIELD [1971], and SOARE [1976].

An ultimate solution for Post's problem would be a complete determination of the structure of $\mathcal{R}$, the countable partially ordered set of r.e. degrees. No such solution is in sight, not even a viable conjecture. The few known results are of a fragmentary nature. A landmark is the *density theorem* of SACKS [1964]: if $a < b$ are r.e. degrees, then there exists an r.e. degree c such that $a < c < b$.

Other results about $\mathcal{R}$ concern its lattice structure. Trivially, $\mathcal{R}$ is an

upper semilattice. Every countable distributive lattice is lattice-embeddable in $\mathcal{R}$ (THOMASON [1971], LACHLAN [1972]). $\mathcal{R}$ itself is not a lattice (LACHLAN [1966], YATES [1966]). Every nonzero r.e. degree is the least upper bound of two smaller r.e. degrees (SACKS [1963]). Not every r.e. degree $< \mathbf{0}'$ is the greatest lower bound of two larger r.e. degrees (LACHLAN [1966]). There exists a pair of nonzero r.e. degrees with greatest lower bound $\mathbf{0}$ (LACHLAN [1966], YATES [1966]). There does not exist a pair of nonzero r.e. degrees with greatest lower bound $\mathbf{0}$ and least upper bound $\mathbf{0}'$ (LACHLAN [1966]). There are a few more results in this vein, due mostly to Lachlan, Yates, and R.W. Robinson. A good survey of the known results is contained in COOPER [1974]. It is not clear where these results are leading.

Nothing is known about automorphisms of $\mathcal{R}$ or about the complexity of the first-order theory of $\mathcal{R}$. SACKS [1963] conjectures that the first-order theory of $\mathcal{R}$ is decidable.

People have often thrashed about looking for meaningful subclasses of the r.e. degrees. The most useful discovery so far has been the following classification according to finite jumps. For $n \in \omega$ we define

$$H_n = \{d \mid d \leq \mathbf{0}' \text{ and } d^{(n)} = \mathbf{0}^{(n+1)}\},$$

$$L_n = \{d \mid d \leq \mathbf{0}' \text{ and } d^{(n)} = \mathbf{0}^{(n)}\}.$$

Degrees in H_1 (L_1) are sometimes called *high* (*low*). The hierarchy $\{H_n, L_n\}_{n \in \omega}$ is known to be proper but not exhaustive: $H_{n+1} - H_n$ and $L_{n+1} - L_n$ each contain r.e. degrees, but there exist r.e. degrees which are not in any H_n or L_n (SACKS [1967]).

Several striking applications of the $\{H_n, L_n\}$ hierarchy are known. We mention here only one type of application. A recursively enumerable set $A \subseteq \omega$ is said to be *maximal* if $\omega - A$ is infinite but there is no recursively enumerable set $B \supsetneq A$ such that both $\omega - B$ and $B - A$ are infinite.

5.1. THEOREM (MARTIN [1966]). *An r.e. degree contains a maximal set if and only if it is H_1 .*

5.2. THEOREM (LACHLAN [1968b], SHOENFIELD [1976]). *An r.e. degree contains a coinfinite recursively enumerable set with no maximal superset, if and only if it is not L_2 .*

Theorems 5.1 and 5.2 bear on the general problem of relating the degree of a recursively enumerable set to its position in the lattice $\mathcal{E}$ of recursively enumerable sets ordered by inclusion. This problem goes back to POST [1944]. Further results on this problem are in SOARE [1974, 1975] where in

particular it is shown that H_n, L_n are not invariant under automorphisms of $\mathcal{E}$.

In recent years, interest has grown in the degrees $\leq 0'$ other than r.e. degrees. One of the basic results here is due to SACKS [1963]: there exists a minimal degree less than $0'$. (By the density theorem for r.e. degrees, no minimal degree can be r.e.) Beautiful refinements of Sacks' theorem have been obtained by Cooper, Yates, R. Epstein, and L. Sasso. For a recent survey of this developing area, see YATES [1974] and the annotated bibliography of COOPER [1974].

YATES [1970, 1972] has announced that every finite distributive lattice is order-isomorphic to a principal ideal $I(a) = \{d \mid d \leq a\}$ such that $a < 0'$. This result implies that the first-order theory of the upper semilattice $I(0')$ is undecidable (see also LACHLAN [1968a], THOMASON [1970]). We conjecture that the first-order theory of $I(0')$ is recursively isomorphic to the truth set of first-order arithmetic (cf. 2.7).

An apparently difficult open problem is whether to every degree $a \leq 0'$ there exists a *relative complement*, i.e. a degree c such that $a \cup c = 0'$ and $a \cap c = 0$. A beautiful result in this direction is:

5.3. THEOREM (ROBINSON [1972]). *If a and b are nonzero degrees $\leq 0'$, then there exists a degree c such that $a \cup c = 0'$ and not $b \leq c$.*

6. Degrees of complete theories

A set $C \subseteq 2^\omega$ is said to be *co-recursively enumerable (co-r.e.)* if $2^\omega - C$ is the domain of a partial recursive functional from 2^ω into ω (see Chapter C.1). The *basis problem* is the problem of effectively choosing an element from a nonempty, co-r.e. subset of 2^ω . In the present section, a number of results on the basis problem will be presented.

The reason for the great interest in the basis problem is that co-r.e. sets often arise naturally in the practice of mathematics. We focus here on a particular class of examples taken from mathematical logic. Let T be a finitely axiomatizable theory in a first-order language of finite similarity type. Assume a fixed Gödel numbering of the sentences of the language of T . A complete theory in this language will be identified with the characteristic function of the set of Gödel numbers of its theorems. Thus the set of all complete extensions of T is identified with a set $C_T \subseteq 2^\omega$. As an abstract topological space, C_T is just the Stone space of the Boolean algebra of sentences of the language of T modulo provable equivalence in T . As a subset of 2^ω , C_T is easily seen to be co-r.e.

We digress to quote the following theorem which shows that the class of examples just discussed is adequate, i.e. comprises essentially all co-r.e. subsets of 2^ω . (Thus, when we study the basis problem in terms of degrees, we are really studying degrees of complete extensions of finitely axiomatizable theories.) Two sets $C_1, C_2 \subseteq 2^\omega$ are said to be *recursively homeomorphic* if there exists a partial recursive functional from 2^ω into 2^ω which maps C_1 one-one onto C_2 .

6.1. THEOREM (HANF [1975]). *Let C be any co-r.e. subset of 2^ω . Then there exists a finitely axiomatizable theory T in the first-order language with equality and one binary relation symbol, such that C is recursively homeomorphic to the set of complete extensions of T .*

In JOCKUSCH and SOARE [1972], priority arguments are used to prove the existence of co-r.e. sets $C \subseteq 2^\omega$ with various pathological properties. We can then apply Theorem 6.1 to deduce corollaries about the existence of finitely axiomatizable theories T with corresponding pathological properties. For more information on this topic see HANF [1965] and MARTIN and POUR-EL [1970].

Our results concerning the basis problem will be stated concisely in terms of a relation $\ll$ on degrees which we now define. A set $C \subseteq 2^\omega$ is said to be co-r.e. in a degree $\mathbf{a}$ if $2^\omega - C$ is the domain of a partial functional from 2^ω into ω which is recursive in $\mathbf{a}$. We put $\mathbf{a} \ll \mathbf{b}$ if every nonempty subset of 2^ω which is co-r.e. in $\mathbf{a}$ contains a function of degree $\leq \mathbf{b}$. The next theorem is a collection of simple facts about $\ll$ whose origins are difficult to trace.

6.2. THEOREM. (i) $\mathbf{a} \ll \mathbf{b}$ implies $\mathbf{a} < \mathbf{b}$.

(ii) $\mathbf{a} \leq \mathbf{b} \ll \mathbf{c} \leq \mathbf{d}$ implies $\mathbf{a} \ll \mathbf{d}$.

(iii) $\mathbf{a} \ll \mathbf{b}$, $\mathbf{b} \ll \mathbf{c}$ implies $\mathbf{a} \ll \mathbf{c}$.

(iv) $\mathbf{a} \ll \mathbf{a}'$ for all $\mathbf{a}$.

The next theorem explains the choice of notation $\ll$.

6.3. THEOREM (JOCKUSCH and SOARE [1972]). *If $\mathbf{a} \ll \mathbf{b}$, then every countable partially ordered set is embeddable in $\{\mathbf{d} \mid \mathbf{a} < \mathbf{d} < \mathbf{b}\}$.*

The next theorem says that there is no positive correlation between $\ll$ and relative recursive enumerability, except as noted in 6.2(iv).

6.4. THEOREM (JOCKUSCH and SOARE [1972]). (i) *If $a \ll b$ and b is r.e. in a , then $a' = b$.*

(ii) *For all a there exists b such that $a \ll b$ and $a' = b'$.*

The next theorem expresses two striking structural properties of $\ll$.

6.5. THEOREM. (i) *If $a \ll b$, then there exists c such that $a \ll c$, $c \ll b$.*

(ii) *For all a and $b \geq a$, there exists $c \gg a$ such that $a = b \cap c$.*

We finish with some results relating $\ll$ to more familiar concepts. For convenience we state the results in unrelativized form. The next theorem is derived from SCOTT [1962], JOCKUSCH and SOARE [1972], and an unpublished result of R.M. Solovay. (See also ROGERS [1967a], p. 94.)

6.6. THEOREM. *For any degree b , the following assertions are pairwise equivalent:*

(i) $b \gg 0$;

(ii) b is the degree of a complete extension of Peano arithmetic (or of ZFC, assuming ZFC is consistent);

(iii) b is the degree of a set which separates an effectively inseparable, disjoint pair of recursively enumerable sets.

6.7. THEOREM (JOCKUSCH [1972]). *For any degree b , the following assertions are equivalent:*

(i) either $b \gg 0$ or $b' \geq 0''$;

(ii) b is the degree of a sequence of functions containing all the recursive elements of 2^ω .

A degree b is said to be *almost recursive* if for every function $p : \omega \rightarrow \omega$ which is recursive in b , there exists a recursive function $q : \omega \rightarrow \omega$ such that $p(n) \leq q(n)$ for all $n \in \omega$. (See also MARTIN and MILLER [1968].)

6.8. THEOREM (JOCKUSCH and SOARE [1972]). *There exists a degree b such that $b \gg 0$ and b is almost recursive.*

References

BOULOS G. and H. PUTNAM

[1968] Degrees of unsolvability of constructible sets of integers, *J. Symbolic Logic*, **33**, 497-513.

BOYD, R., G. HENSEL and H. PUTNAM

[1969] A recursion-theoretic characterization of the ramified analytical hierarchy, *Trans. Am. Math. Soc.*, **141**, 37-62.

COOPER, S.B.

[1973] Minimal degrees and the jump operator, *J. Symbolic Logic*, **38**, 249–271.

[1974] An annotated bibliography for the structure of the degrees below $0'$ with special reference to that of the recursively enumerable degrees, *Recursive Function Theory Newsl.*, **5**, 1–15.

DAVIS, M., editor

[1965] *The Undecidable* (Raven Press, New York).

FRIEDBERG, R.M.

[1957a] Two recursively enumerable sets of incomparable degrees of unsolvability (solution of Post's problem 1944), *Proc. Nat. Acad. Sci. U.S.A.*, **43**, 236–238.

[1957b] A criterion for completeness of degrees of unsolvability, *J. Symbolic Logic*, **22**, 159–160.

GÖDEL, K.

[1939] Consistency proof for the generalized continuum hypothesis, *Proc. Nat. Acad. Sci. U.S.A.*, **25**, 220–224.

HANF, W.

[1965] Model theoretic methods in the study of elementary logic, in: *Theory of Models*, edited by J.W. Addison et al. (North-Holland, Amsterdam) pp. 132–145.

[1975] The Boolean algebra of logic, *Bull. Am. Math. Soc.*, **81**, 587–589.

JENSEN, R.B.

[1972] The fine structure of the constructible hierarchy, *Ann. Math. Logic*, **4**, 229–308.

JOCKUSCH, C.G., JR.

[1972] Degrees in which the recursive sets are uniformly recursive, *Canad. J. Math.*, **24**, 1092–1099.

JOCKUSCH, C.G., JR. and S.G. SIMPSON

[1976] A degree-theoretic definition of the ramified analytical hierarchy, *Ann. Math. Logic*, **10**, 1–32.

JOCKUSCH, C.G., JR. and R.I. SOARE

[1972] π_1^0 classes and degrees of theories, *Trans. Am. Math. Soc.*, **173**, 33–56.

KLEENE, S.C. and E.L. POST

[1954] The upper semilattice of degrees of recursive unsolvability, *Ann. of Math.*, **59**, 379–407.

LACHLAN, A.H.

[1966] Lower bounds for pairs of recursively enumerable degrees, *Proc. London Math. Soc.*, **16**, 537–569.

[1968a] Distributive initial segments of the degrees of unsolvability, *Z. Math. Logik Grundlagen Math.*, **14**, 457–472.

[1968b] Degrees of recursively enumerable sets which have no maximal superset, *J. Symbolic Logic*, **33**, 431–443.

[1972] Embedding nondistributive lattices in the recursively enumerable degrees, in: *Conference in Mathematical Logic — London 1970*, Lecture Notes in Mathematics, Vol. 255 (Springer, Berlin) pp. 149–177.

[1973] The priority method for the construction of recursively enumerable sets, in: *Cambridge Summer School in Mathematical Logic*, Lecture Notes in Mathematics, Vol. 337 (Springer, Berlin) pp. 299–310.

LACHLAN, A.H. and R. LEBEUF

[1976] Countable initial segments of the degrees of unsolvability, *J. Symbolic Logic*, **41**, 289–300.

LERMAN, M.

[1971] Initial segments of the degrees of unsolvability, *Ann. of Math.*, **93**, 365–389.

- MARTIN, D.A.
 [1966] Classes of recursively enumerable sets and degrees of unsolvability, *Z. Math. Logik Grundlagen Math.*, **12**, 295–310.
 [1968] The axiom of determinateness and reduction principles in the analytical hierarchy, *Bull. Am. Math. Soc.*, **74**, 687–689.
 [1970] Measurable cardinals and analytic games, *Fund. Math.*, **66**, 287–291.
 [1975] Borel determinacy, *Ann. of Math.*, **102**, 363–371.
- MARTIN, D.A. and W. MILLER
 [1968] The degrees of hyperimmune sets, *Z. Math. Logik Grundlagen Math.*, **14**, 159–166.
- MARTIN, D.A. and M.B. POUR-EL
 [1970] Axiomatizable theories with few axiomatizable extensions, *J. Symbolic Logic*, **35**, 205–209.
- MUCHNIK, A.A.
 [1956] On the unsolvability of the problem of reducibility in the theory of algorithms (in Russian), *Dokl. Akad. Nauk SSSR*, **108**, 194–197.
- POST, E.L.
 [1944] Recursively enumerable sets of positive integers and their decision problems, *Bull. Am. Math. Soc.*, **50**, 284–316. (Reprinted in DAVIS [1965].)
 [1948] Degrees of recursive unsolvability (preliminary report), *Bull. Am. Math. Soc.*, **54**, 641–642.
- ROBINSON, R.W.
 [1972] Degrees joining to $\mathbf{0}'$, unpublished manuscript, 12 pp.
- ROGERS, H. JR.
 [1967a] *Theory of Recursive Functions and Effective Computability* (McGraw-Hill, New York) 482 pp.
 [1967b] Some problems of definability in recursive function theory, in: *Sets, Models, and Recursion Theory*, edited by J.N. Crossley (North-Holland, Amsterdam) pp. 183–201.
- SACKS G.E.
 [1963] Degrees of Unsolvability, *Ann. Math. Studies*, **55**, 174 pp.
 [1964] The recursively enumerable degrees are dense, *Ann. of Math.*, **80**, 300–312.
 [1967] On a theorem of Lachlan and Martin, *Proc. Am. Math. Soc.*, **18**, 140–141.
 [1971] Forcing with perfect closed sets, in: *Axiomatic Set Theory*, edited by D. Scott, Proceedings of Symposia in Pure Mathematics, Vol. 13 (Am. Math. Soc., Providence, RI) pp. 331–355.
- SCOTT, D.
 [1962] Algebras of sets binumerable in complete extensions of arithmetic, in: *Recursive Function Theory*, edited by J. Dekker, Proceedings of Symposia in Pure Mathematics, Vol. 5 (Am. Math. Soc., Providence, RI) pp. 117–121.
- SHOENFIELD, J.R.
 [1965] Applications of model theory to degrees of unsolvability, in: *The Theory of Models*, edited by J.W. Addison et al. (North-Holland, Amsterdam) pp. 359–363.
 [1967] *Mathematical Logic* (Addison-Wesley, Reading, MA) 344 pp.
 [1971] *Degrees of Unsolvability* (North-Holland, Amsterdam) 111 pp.
 [1976] Degrees of classes of r.e. sets. *J. Symbolic Logic*, **41**, 695–696.
- SIMPSON, S.G.
 [1975] Minimal covers and hyperdegrees, *Trans. Am. Math. Soc.*, **209**, 45–64.
 [1977] First-order theory of the degrees of recursive unsolvability, *Ann. of Math.*, to appear.
- SOARE, R.I.
 [1974] Automorphisms of the lattice of recursively enumerable sets, *Bull. Am. Math. Soc.*, **80**, 53–58.

- [1975] Incomplete recursively enumerable sets, *Notices Am. Math. Soc.*, **22**, A-24.
 - [1976] The infinite injury priority method, *J. Symbolic Logic*, **41**, 513-530.
- SPECTOR, C.
- [1956] On degrees of recursive unsolvability, *Ann. of Math.*, **64**, 581-592.
- THOMASON, S.K.
- [1970] On initial segments of hyperdegrees, *J. Symbolic Logic*, **35**, 189-197.
 - [1971] Sublattices of the recursively enumerable degrees, *Z. Math. Logik Grundlagen Math.*, **17**, 273-280.
- YATES, C.E.M.
- [1966] A minimal pair of recursively enumerable degrees, *J. Symbolic Logic*, **31**, 159-168.
 - [1970] Initial segments of the degrees of unsolvability, Part I: a survey, in: *Mathematical Logic and the Foundations of Set Theory*, edited by I. Bar-Hillel (North-Holland, Amsterdam) pp. 63-83.
 - [1972] Initial segments and implications for the structure of degrees, in: *Conference in Mathematical Logic — London 1970*, Lecture Notes in Mathematics, Vol. 255 (Springer, Berlin) pp. 305-335.
 - [1974] Prioric games and minimal degrees below $0'$, *Fund. Math.*, **82**, 217-237.
 - [1976] Banach-Mazur games, comeager sets, and degrees of unsolvability, *Math. Proc. Camb. Phil. Soc.*, **79**, 195-220.

α -Recursion Theory

RICHARD A. SHORE*

Contents

Introduction	654
1. Ideas and definitions	655
2. Questions and answers	659
3. An example	662
4. Interactions and applications	667
5. Bibliographic guide	670
Annotated bibliography	671

* The chapter is based on an invited address given to the Association of Symbolic Logic at its annual meeting at Washington, D.C. in January of 1975. Its preparation was partially supported by NSF grant MSP 74-06378. The author also wishes to thank B. Dreben, C. Jockusch, G. Kreisel, S. Kripke, A. Leggett, M. Lerman, A. Nerode and G. Sacks for helpful conversations and correspondence.

Introduction

Our goal in this chapter is to give the non-specialist a rough picture of the current state of α -recursion theory (i.e., recursion theory on admissible ordinals). We hope first (Section 1) to explain the basic ideas underlying the subject and then (Section 2) to present the important questions and main areas of research currently being pursued. We will also report on the progress being made and on the techniques being developed and employed in this work. To illustrate these ideas we will (Section 3) give one fairly complete proof of a typical theorem in α -recursion theory and then (Section 4) examine the relation and application of these methods to other areas of research. Of necessity our treatment of the historical background as well as the material itself will be both sketchy and superficial. We have tried to include a fairly complete and somewhat annotated bibliography to help fill in the gaps.

Historically the motivation for generalizing recursion theory to infinite ordinals came from the several branches of mathematical logic: proof theory, model theory and set theory as well as, of course, recursion theory itself. Thus, for example, TAKEUTI [1954, 1957] was interested in the problem of reducing the consistency of set theory to that of a theory of ordinal numbers. In TAKEUTI [1960] he introduced a recursion theory on the ordinals to show that the required theory and relative consistency proof could be made effective in some generalized sense. Essentially he showed that Gödel's construction of L (the class of constructible sets) could be mimicked in an (ordinal) effective way to give a (recursively) isomorphic copy of L within his theory of ordinal numbers (TAKEUTI [1965a]). In many ways this work foreshadowed the close interconnections between recursion theory and set theory that arose in the study of the fine structure of L . We will discuss this relationship at some length later on.

In the model-theoretic vein we cite two examples. MACHOVER [1961] (who also collaborated with Levy) wanted to generalize model-theoretic ideas and results which involved recursion-theoretic concepts to the infinitary languages $I_{\kappa, \kappa}$. He therefore developed a recursion theory on regular infinite cardinals to state and prove such theorems as satisfiability is not "arithmetically" definable. In a somewhat different vein we have the work of KREISEL [1961, 1965] (who later collaborated with Sacks in KREISEL and SACKS [1963, 1965]). The main interest here seems to be definability theory and its relation to various higher logics and languages. This work developed along both recursion-theoretic lines (as evidenced in the papers with Sacks) which we will continue to discuss and more model-theoretic

ones (although with some proof-theoretic flavorings as well). The latter stemmed from Kreisel's insistence on restrictions of infinitary language and associated generalizations of finiteness based on definability considerations rather than cardinality. In the hands of Barwise and others it has flowered into the extensive subject of admissible structures and their associated infinitary languages. As this area lies outside the scope of this chapter we will only refer the reader to the bibliography for some starting points in the literature and to Chapter A.7.

The set-theoretic viewpoint is represented by the work of Jensen in JENSEN and KARP [1971]. (Karp, however, came to the subject from a model-theoretic approach, somewhat like Machover's.) As this approach is intimately connected with the recursion-theoretic one represented by KRIPKE [1964a, 1964b] and PLATEK [1966] (as well as the previously mentioned work of Kreisel and Sacks), which forms the heart of our subject, we will try to follow developments from both points of view.

In addition to the specific problems from other areas that motivated the early work on recursion theory on ordinals, there were also general principles involved. The recursion theorists had many of the usual goals of generalization in mind. One hopes to build not only new and interesting abstract structures but also ones that will illuminate ordinary recursion theory and perhaps prove useful in applications as well. A further hope is that such work might lead to an axiomatic approach to recursion theory. The set-theorist, on the other hand, comes to the subject with the goals of effectivization rather than generalization. By introducing notions of effectiveness he hopes to gain a finer and deeper knowledge of the structure of sets and eventually to exploit this extra information to solve already existing problems in set theory.

1. Ideas and definitions

The question now is where to begin a generalization of recursion theory. One must first decide what are the basic objects and notions in ordinary recursion theory that one wishes to generalize or abstract. Of course we have the natural numbers $0, 1, 2, 3, \dots$ as the primary elements of our universe, while the basic notions of interest seem to be recursiveness and recursive enumerability. One natural generalization for the numbers is certainly the ordinals. After all one just keeps on counting past ω . One has, however, two choices corresponding, perhaps, to two different views of the natural numbers. One can take either all the ordinals (ON) or just some

initial segment of ordinals up to say α as the basic objects. We will concentrate on the latter approach, though most of what we say will apply equally well to both. As for definitions of recursiveness and recursive enumerability, the recursion theorist has several standard alternative approaches to consider (though in ordinary recursion theory all of them define the same class of functions). Many of these schemes were tried out by the early workers in the field. To cite some examples we note that TAKEUTI [1960] introduced schemes for generating semi-recursive functions and with KINO [1962] put forth an alternate approach that first generated primitive recursive functions and then applied a μ (least number) operator. Other proposals included analogs of Turing machines (LEVY [1963]), definability criteria (KREISEL [1965]) and various types of equation calculi (MACHOVER [1961], TUGUÉ [1964] and KRIPKE [1964a]).

The most useful approach seems to be one based on an equation calculus like that in KRIPKE [1964a]. One takes Kleene's ordinary equation calculus and adds on an infinitary rule that expresses the underlying idea of the generalization: one is to be allowed up to α many steps in a computation and to survey up to α many bits of information so far produced at each of these steps (see KRIPKE [1967] or SACKS [1967] for further discussion and technical details).¹ One then defines the recursive functions as usual to be those whose values can be consistently deduced from some finite set of equations via these rules. The recursively enumerable (r.e.) sets are, of course, the ones which can be recursively listed. (We will indicate the generalized notions by prefixing an α as in " α -recursive" and " α -recursively enumerable".)

One problem immediately comes to mind with this procedure. Not all ordinals α will be satisfactory domains for this recursion theory. Thus for example $\omega + 17$ is not closed under addition and should surely be unacceptable. Whatever procedure we use for defining recursiveness, we want at the very least to guarantee that α be closed under recursive functions. Thinking specifically in terms of an equation calculus we would also want to require that any individual computation, i.e. deduction, of the value of some recursive function be completed in fewer than α many steps. Both of these requirements are met if we assume that for any given finite set of

¹ We should remark that some care is needed in the choice of an equation calculus. Kripke told us in the name of A. Levy (see Avot 6:6) that the system of MACHOVER [1962] has problems if $V \neq L$ because of the use of infinitely many variables and the supremum operator. Indeed, even if one uses only finitely many variables and assumes $V = L$, the formulations using the sup or lub operator of TUGUÉ [1964] and STILLWELL [1970] have all the desired properties only for regular cardinals.

equations all possible consequences can be deduced in fewer than α many steps. Such ordinals are called *admissible* (KRIPKE [1964a]) and constitute the proper domains for our recursion theories. (We should note that it was not until the work of KRIPKE [1964a] and PLATEK [1966] that the proper domains for recursion theory on ordinals were isolated. Most of the other workers (e.g. MACHOVER [1961], LEVY [1963] and TUGUÉ [1964]) restricted their attention to the obviously suitable case of regular cardinals. That other domains were possible was realized in TAKEUTI [1960], where it was shown that singular cardinals as well were closed under recursive functions. In addition KREISEL and SACKS [1965], approaching matters in a quite different manner, worked on ω_1^{ck} , the least non-recursive ordinal which is also the least admissible after ω .)

Although it may not be obvious, there is another basic notion that requires generalization: finiteness. Early work tended to leave it unchanged or (especially in infinitary languages) employ cardinality conditions (sets of size $< \alpha$ were α -finite). The need for a finer approach was first stressed in KREISEL [1961]. In our present setting it would certainly seem reasonable to require that each of our counting numbers (the ordinals less than α) be considered α -finite. This, however, would not be enough. What would we say of sets which were the same size as some $\beta < \alpha$? Surely if the correspondence between elements were effective it too would be α -finite. Is this, however, sufficient? As it turns out it helps to turn to a set-theoretical viewpoint to answer this question. Let us therefore consider for a moment how a set-theorist might generalize recursion theory into the infinite.

A natural starting point for someone interested in effectivizing set theory is Gödel's constructible universe (see Chapter B.5). It, after all, consists of those sets built by the most effective method of ordinary set theory — definition. Again we have here two choices for our domain of discourse. We can work with all of L or with some initial segment L_α (the sets constructed by level α). As before we will concentrate on the latter alternative mostly for the sake of notational convenience. Given such a domain L_α built up by definitions, it seems reasonable to look at complexity of definition as a guide to deciding which subsets of, or functions on, L_α are to be considered simple or effective. If we combine this idea with the one that a recursively enumerable set is one given by a search operation or enumeration, then a good candidate for recursive enumerability is being Σ_1 over L_α (i.e. definable by a formula with parameters in L_α and a single initial existential quantifier as the only quantifier not restricted in its scope to an element of L_α). The idea of

course is that an element is put in a Σ_1 set when we find (in our search through L_α) a witness for the existential quantifier. (Checking the truth of such a sentence only involves looking inside a single element (say an L_β for $\beta < \alpha$) of L_α and so is surely effective.) With a definition of recursive enumerability at hand we can define a subset of L_α to be recursive if both it and its complement are r.e. (i.e. it is Δ_1).

We are again faced with the problem that not all ordinals α will correspond to an L_α suitable for our recursion theory. Thinking now as set-theorists we might try to remedy this situation by requiring that L_α satisfy the axioms of set theory in some effective form. In particular this means that in addition to the usual trivial axioms (extensionality, empty set, pairing and union) which are satisfied by any L_λ , with λ a limit, we might ask that the replacement axiom (or equivalently the Aussonderung axiom) hold for effective functions ($= \Delta_1 = \Sigma_1$ with domain an element of L_α). We do however give up the power set axiom entirely. As it turns out this requirement of Σ_1 -replacement is equivalent to the recursion-theoretically defined notion of admissibility (see KRIPKE [1964a] or FUKUYAMA [1971] for the actual details of the equivalence). Thus we see the beginnings of the relationship between the two approaches.

The connection between these two formulations is in fact much more thoroughgoing than this one coincidence. Indeed they are essentially the same. For admissible α there is an α -recursive relation on α which is isomorphic to the $\in$ relation on L_α . Moreover, all the basic notions are carried over by the translation. Thus a set is α -recursive, or α -r.e., iff its image is Δ_1 or Σ_1 over L_α respectively. This equivalence can be used to guide us to a good answer to our question about the proper definition for α -finite. For the set-theorist the natural generalization of finite to element of L_α makes good sense. Upon translating this back to recursion-theoretic language we discover that it is equivalent to being the recursive image of an ordinal less than α . This equivalence is then good evidence for the adequacy of our definition of α -finite.

We should also point out that when this problem of generalized finiteness was first raised by Kreisel it was with special emphasis on the analogy between Π_1^1 and r.e. in ordinary recursion theory. The proposal (KREISEL [1961]) was to have Δ_1^1 correspond to finite rather than recursive to improve the analogy. When KREISEL and SACKS [1963, 1965] formulated these ideas in terms of recursion theory on ω_1^{ck} they accordingly generalized finite to recursive and bounded. (Π_1^1 sets indeed become ω_1^{ck} -r.e. and so Δ_1^1 subsets of ω were ω_1^{ck} -recursive and bounded.) This definition is also easily seen to be equivalent to that of α -finite.

2. Questions and answers

Now that we have agreed on the primary notions of α -recursion theory we must consider what sort of questions should be attacked. After establishing the basic facts of ordinary recursion theory, such as the enumeration, iteration and recursion theorems, the recursion-theorist is naturally drawn to the traditional areas of investigation of ordinary recursion theory: relative complexity (that is degree theory) particularly of the r.e. sets and structural (that is lattice-theoretic) properties of sets, again usually of the r.e. sets. These areas have recently constituted the major concerns of α -recursion theory. In addition to establishing the main structural theorems (for degrees as well as sets), the goal of much of the current work has been to analyze and illuminate the methods used in these areas. In particular the various types of priority arguments that are the key to most of the deeper results of ordinary recursion theory have been extensively studied and adapted to the general setting of α -recursion theory. We will just mention some of the results in each area, but we must first pause to explain what we mean by α -degrees and α -reducibilities.

There are a number of different reducibilities of interest in ordinary recursion theory. Some of them such as many-one and one-one reducibilities have useful straightforward generalizations in α -recursion theory: $A \leq_{m\alpha} B$ ($A \leq_{1-\alpha} B$) iff there is a (one-one) α -recursive function f such that $\beta \in A \Leftrightarrow f(\beta) \in B$. On the other hand the situation for Turing reducibility (which is certainly the most important one in ordinary recursion theory) is somewhat more complicated.

Perhaps the most common approach now to Turing reducibility is in terms of an oracle. One views a computation relative to some function f (sets are considered in terms of their characteristic functions) as proceeding along as usual with the added proviso that at any point one may obtain from the oracle the value of f at a given number n . In terms of the equation calculus we might first try to put all of f into the initial set of equations, for then at any step we have available the value of $f(n)$ for each n . We would then say that g is computable from f if all its values can be consistently deduced from a finite set of equations plus the complete graph of f . In α -recursion theory this defines the reducibility called α -calculability. (We write $g \leq_{c\alpha} f$ ($A \leq_{c\alpha} B$) to mean that $g(A)$ is α -calculable from $f(B)$.)

Although α -calculability is an important and useful reducibility (for countable α it corresponds to KREISEL'S [1965] model-theoretically defined notion of implicit invariant definability), we do not consider it the appropriate recursion-theoretic one. Its principal conceptual shortcomings

are that a single computation of a value of g may use α -infinitely much information about f and may take more than α many steps to complete. Both of these possibilities seriously conflict with our intuitive ideas from ordinary recursion theory about how relative computations should proceed.

To see how to overcome these difficulties we turn to another view of relative recursiveness in ordinary recursion theory which incorporates these intuitions. The idea is that we should be able to specify the computation procedure effectively along with the questions it asks of the oracle in any given computation. That is, the description of the procedure as a whole is independent of the particular answers given along the way. One can picture the procedure as being given by an effective tree structure, branching at the various questions. The information used on any terminating path is then the finite amount needed for that computation. We recommend ROGERS [1967] pp. 128–132, who takes this approach as basic in ordinary recursion theory, for further discussion. We think of the computation procedure as being coded by an r.e. set. This set enumerates terms corresponding to the outputs of terminating branches paired with the finite set of answers needed to produce those outputs. This view leads us to a reasonable formal definition: A is α -recursive in B , written $A \leq_\alpha B$, iff there is an α -r.e. set W_e such that for each α -finite set K we have that

$$K \subseteq A \Leftrightarrow \exists \langle K, 1, M, N \rangle \in W_e (M \subseteq B \ \& \ N \subseteq \bar{B}),$$

$$K \subseteq \bar{A} \Leftrightarrow \exists \langle K, 0, M, N \rangle \in W_e (M \subseteq B \ \& \ N \subseteq \bar{B})$$

where M and N range over α -finite sets and we employ some effective coding scheme for such sets and quadruples. Note that, in line with our generalizing the concept of finiteness, both our inputs (M, N) and outputs $(K \subseteq A \text{ or } K \subseteq \bar{A})$ are required to be α -finite. (Historically an earlier attempt at a definition only asked for single (or equivalently truly finite) outputs. This is now called weak α -recursiveness — $A \leq_{w\alpha} B$. Not only does this fail to capture the true spirit of the generalization but it turns out (DRISCOLL [1968]) to be technically unworkable as a reducibility — it is not transitive.)

Associated with this reducibility ($\leq_\alpha$) we naturally have a notion of α -degree (the equivalence classes under $\leq_\alpha$ are generally denoted by bold-face letters $\mathbf{a}, \mathbf{b}, \mathbf{c}, \dots$). The degrees are given the structure of an upper-semilattice by the ordering induced by $\leq_\alpha$ and the join operator $\vee$ defined as in ordinary recursion theory. As we said before, the investigation of the structure of this semilattice has been one of the main areas of research in

α -recursion theory (mostly by Sacks and his students). The most successful work in terms of the methodology of priority arguments as well as actual structural results has been on the α -degrees of α -r.e. sets (called the α -recursively enumerable degrees). Although much work had previously been done for certain ordinals (especially ω_1^{ck}), the first real success of the priority method for all admissibles came when SACKS and SIMPSON [1972] established the analog of the Friedberg–Muchnik solution to Post’s problem: there are incomparable α -r.e. degrees, that is, degrees a and b such that $a \not\leq_\alpha b$ and $b \not\leq_\alpha a$. They achieved more, however, than merely solving this problem. Their methods were sufficient to handle all types of simple finite injury priority arguments for all admissible ordinals.

Since then considerable progress has been made with more difficult priority arguments. The methods developed in SHORE [1975a] to prove the splitting theorem (for every non- α -recursive α -r.e. c there are α -r.e. a and b such that $a \leq_\alpha c$, $b \leq_\alpha c$ and $a \vee b = c$) seem adequate for priority arguments with unbounded preservations (see Section 3 below for details). The status of infinite injury arguments in α -recursion theory is somewhat less clear at the moment. The prime example from ordinary recursion theory has been successfully generalized — the α -r.e. degrees are dense (SHORE [1976a]) — but not all the theorems investigated have worked out so well. Thus for example LERMAN and SACKS [1972] showed that there is a minimal pair of α -r.e. degrees (i.e. non- α -recursive α -r.e. a and b such that if $c \leq_\alpha a$ and $c \leq_\alpha b$ then c is the degree of the α -recursive sets) for most but not all admissible α . (A slight improvement is given in SHORE [1975b] but the most difficult case remains open.)

Along these lines the main open question seems to be to find a first order difference between the theory of the r.e. degrees and that of the α -r.e. degrees for some α . Indeed this question is open even for the theory of all α -degrees. The only answer (to either question) currently available uses the jump operator: thus for example if $\alpha = \aleph_\omega^L$ and $A \leq_\alpha 0'$, then $A' \equiv_\alpha 0'$ (SHORE [1976b]), while in ordinary recursion theory there are even r.e. sets $A \leq 0'$ with $A' \equiv 0''$ (SACKS [1966a], §7). Of course the real point is to find a difference in the theories with only $\leq$ in the language.¹ We must admit, however, that very little is known at all about the structure of the α -degrees as a whole. Even the first question one might ask has not been completely answered: minimal α -degrees are known to exist for all countable α (MACINTYRE [1974]) and all Σ_2 admissibles (SHORE [1972b]) but not in general for every α . The prime example of the unknown cases is $\alpha = \aleph_\omega^L$.

¹ (Added in proof.) Such a difference has now been found, see SHORE [1976c].

The other major area of current research has been the structure of the lattice of α -r.e. sets, $\mathcal{E}(\alpha)$ (mainly by Lerman and his students). In addition to illuminating the structure of the α -r.e. sets by answering specific natural questions about the lattice (e.g. are there maximal elements), the overall goal of this work has been to settle the question of the decidability of these lattices. Although this is a major open problem even in ordinary recursion theory, it is hoped that one will be able to attack it piecemeal for various α 's which have especially simple lattice structures.

To be more precise, as in ordinary recursion theory one's attention really centers on the lattice $\mathcal{E}^*(\alpha)$ of α -r.e. sets modulo "finite" sets. What should be a fruitful analog for finiteness in this setting has itself been a matter for some investigation as in LERMAN [1976b, 1976c]. For lattice-theoretic purposes the best choice seems to be what Lerman calls α^* -finite (the set and all its α -r.e. subsets are α -finite). This notion is the only one giving an ideal of generalized finite sets which is definable over $\mathcal{E}(\alpha)$. Moreover the theory of $\mathcal{E}(\alpha)$ is equidecidable with that of the quotient lattice $\mathcal{E}^*(\alpha)$ (LERMAN [1976b]).

In line with the general goal of attacking the decidability of $\mathcal{E}^*(\alpha)$ for various α , work has been directed not only at proving general theorems for all admissibles but also at analyzing it in depth for certain promising ones such as $\aleph_1^L$ and $\aleph_\omega^L$. The best result of the first sort is LERMAN's [1974a] characterization of those admissibles which have maximal elements in $\mathcal{E}^*(\alpha)$. Essentially he shows that this happens if and only if α is countable via a function with a certain type of recursive approximation. (The necessity of some countability assumption was first shown in LERMAN and SIMPSON [1973].) For examples of the second type of result we here cite work by CHONG and LERMAN [1975] on hyperhypersimple sets (ones whose supersets in $\mathcal{E}^*(\alpha)$ form a Boolean algebra) and of LERMAN [1976a] and LEGGETT and SHORE [1976] on the possible 1-types of simple sets (ones whose complement, although α^* infinite, contain no α^* infinite α -r.e. subset). Needless to say much work remains to be done in this area.¹

3. An example

Work in α -recursion theory has shed some light on the general nature of priority arguments and generated applications to both recursion in higher type objects (HARRINGTON [1973]) and axiomatic recursion theory (SIMPSON [1974b]). It has also interacted with set-theoretic work in a strong way. Perhaps the best way to explain both these relationships and the workings

¹ (Added in proof.) See LERMAN [1977] for some major progress.

of α -recursion theory itself is by an example. We will present a slightly modified proof of the *Splitting Theorem* from SHORE [1975a]. We first sketch the proof of this theorem in ordinary recursion theory (see SACKS [1966a], § 5, or SHOENFIELD [1971], §14).

THEOREM. *Let C be an r.e. member of a given non-recursive r.e. degree c enumerated by c . We wish to construct r.e. sets A and B such that $A \cup B = C$, $A \cap B = \emptyset$, $A \leq_T C$, $B \leq_T C$, $C \not\leq_T A$ and $C \not\leq_T B$.*

(Notice that $A \cup B = C$ implies that $A \vee B \equiv_T C$ and so we have split the degree of C as required.) The basic plan is, at each stage σ of the construction, to put $c(\sigma)$ into precisely one of A and B (the positive requirements). This immediately insures that $A \cup B = C$, $A \cap B = \emptyset$, $A \leq_T C$ and $B \leq_T C$ (to see if $x \in A$, say, ask if $x \in C$ and if so wait until it is enumerated and check whether or not it is put into A). Thus we only have to take steps to make sure that we cannot compute C from A or B . Our (somewhat roundabout) approach here (due to Sacks) is that for each e we attempt (with priority e) to preserve computations of $\{e\}^A$ (and similarly $\{e\}^B$) on initial segments as long as they seem to agree with C (i.e. its characteristic function). The idea is that once e has highest priority (as explained below) we preserve the first available computation of $\{e\}^A(x)$ for each x as long as we have no disagreement with C . If $\{e\}^A = C$ we would thus preserve such computations for every x . Of course $\{e\}^A$ would then be recursive. (Just wait until we preserve a computation $\{e\}^A(x)$. As e has highest priority it will never be destroyed and so will give the correct value of $\{e\}^A$.) We then would contradict the non-recursiveness of C .

To be precise, the construction and the simultaneous definition of terminology proceeds as follows: We let A^σ and C^σ denote the elements enumerated in A and C before stage σ respectively. We use the notation $\{e\}_\sigma^A(x) = C^\sigma(x)$ to mean that there is a computation (the appropriate 4-tuple) less than σ which shows that computing via procedure e relative to A^σ at x gives the characteristic function of C^σ at x . At stage σ we find, for each e -active $x < \sigma$, the least computation of $\{e\}_\sigma^A(x) = C^\sigma(x)$ (if one exists) and create a negative e -requirement for A with argument x consisting of the elements assumed to be outside of A in this computation (where x is the least number y for which we now have no negative e -requirement with argument y). If at any later stage we put an element of this requirement into A we say that we have *destroyed* it. We say that a reduction procedure $e < \sigma$ is e -active at stage σ unless we have a negative e -requirement (as yet undestroyed) with argument y such that $\{e\}_\sigma^A(x) \neq C^\sigma(y)$ (note that this can only happen if y has been enumerated in C since the requirement

was created) in which case it is *inactive*. Of course we do all of this for B as well.

Finally we put $c(\sigma)$ into A or B so as to preserve as much as possible. That is, we let e_A (e_B) be the least number such that $c(\sigma)$ belongs to a negative e -requirement for A (B) (say -1 if there is no such number). If $e_A \leq e_B$ we put $c(\sigma)$ into B ; otherwise it goes into A . Thus we have given e requirements for A priority over e' ones for B iff $e \leq e'$.

To see that the construction succeeds (i.e. $C \not\leq_T A$ and $C \not\leq_T B$) one first argues by induction on e that only finitely many negative e -requirements are ever created.

Suppose, for the sake of induction, that by stage σ_0 we have created all negative e' -requirements for $e' < e$ that will ever be created. Together they all form a finite set, say N . By some stage $\sigma_1 \geq \sigma_0$ all elements of $C \cap N$ will have been enumerated in C . The priority ordering now guarantees that any e -requirement for A created after stage σ_1 is never destroyed. (We call such requirements *permanent* and others *temporary*.) Note first that if at any stage $\sigma > \sigma_1$ e is inactive, it is inactive forever after, as the associated requirement is permanent. Thus, by the rules of the construction, no further e -requirements for A can ever be created. If, however, e is never inactive at a stage $\sigma > \sigma_1$, then by definition every e requirement for A is associated with a computation $\{e\}^A(x)$ giving the correct value of $C(x)$. As such requirements are created for initial segments of x 's there can be infinitely many of them only if we create one for each x . Were this the case, however, we could compute $C(x)$ by just looking at the value of the first e -requirement for A with argument x created after stage σ_1 . As this would contradict the non-recursiveness of C , we conclude that there are only finitely many e -requirements ever created for A . We then argue similarly for B .

It is now fairly easy to see that $C \not\leq_T A$. Suppose that $\{e\}^A = C$ and let σ_1 be as in the above argument. e can never be inactive at any stage $\sigma > \sigma_1$ for then $\{e\}^{A^\sigma}(x) \neq C^\sigma(x)$ (with $x \in C$ in fact) and the permanence of the requirement implies that this computation from A is correct contradicting $\{e\}^A = C$. Thus nothing prevents us from creating e -requirements for A with argument x for each x when the correct computation of $\{e\}^A(x) = C(x)$ actually turns up. Of course, this contradicts the above result that all these requirements are finite and so $C \not\leq_T A$. Of course $C \not\leq_T B$ by the same argument.

Let us now try to follow the same procedure in α -recursion theory. The only difficulties appear in the inductive proof that there are only α -finitely many e -requirements for each e . The major difficulty is one endemic in

α -recursion theory. Even if we have proven this for *each* $e' < e$ we do not know that the set N of *all* such requirements is α -finite. We cannot therefore assume the existence of a stage σ_0 as required. The point is that a union of fewer than α many α -finite sets need not be α -finite. For example if $\alpha = \aleph_\omega$ nothing prevents the formation of e -requirements for every $x < \aleph_e$ for each $e < \omega$. Thus we would have α many e' -requirements for $e' < \omega$ and no stage like σ_0 would exist. (Note that if N is α -finite σ_0 does exist since the map, taking an element of N to the stage at which it is created, is α -recursive and so bounded on α -finite sets by admissibility.)

The only other apparent problem is that even if N is α -finite $C \cap N$ need not be and so there could be no stage σ_1 as in the original argument. (Again note that if $C \cap N$ is α -finite it is enumerated in α -finitely many steps by admissibility.) Although this too is a common problem in α -recursion theory, SACKS [1966c] has supplied an easy remedy. We call a set C *regular* if $C \cap N$ is α -finite for every α -finite N . What SACKS [1966c] tells us is that every α -r.e. degree contains a regular α -r.e. set. Thus with no loss of generality we may assume that C is regular and so eliminate the second problem.

The key to solving the first problem comes from SHORE [1975a, 1976a]. The idea is to make the list of negative requirements so short that the problem can never arise. For example if $\alpha = \aleph_\omega$ we would like to limit ourselves to an ω -list. In general the bound on the creation of e -requirements (if it exists) is given by a Σ_2 function. Thus we want to arrange the priority ordering e of reduction procedures in a list of length γ such that there is no Σ_2 map on any $\delta < \gamma$ which is unbounded in α . The greatest such γ (and so the most likely choice) is called the Σ_2 cofinality of α ($\sigma 2cf(\alpha)$). To accomplish this we block the reduction procedures into $\gamma = \sigma 2cf(\alpha)$ many pieces $\{B_e\}_{e < \gamma}$, each a proper initial segment of the usual list of reduction procedures (thus for $\alpha = \aleph_\omega$ we would have $B_e = \aleph_e$ for $e < \omega$). The idea is, for each x , to accept computations of $\{\delta\}^{A^\sigma}(x) = C^\sigma(x)$ from any $\delta \in B_e$. We should also note that we can generate these blocks via a recursive approximation which will be correct on each initial segment of γ from some point on. (We use the usual approximation from ordinary recursion theory for total Σ_2 (and so Δ_2) functions. The admissibility of α makes the approximation converge pointwise and the convergence on initial segments is assured by γ 's being the Σ_2 cofinality of α .)

All that really remains to be checked is that this blocking does not interfere with computing C if there are α -infinitely many e -requirements for some $e < \gamma$. This, however, presents one more important problem that we must deal with before we can precisely formulate our construction.

Consider some B_e and assume that as in the ordinary proof we have a stage σ_1 such that no e -requirement for A is ever destroyed after σ_1 . In order to compute C , given that there are α -infinitely many e -requirements, we must eliminate those $\delta \in B_e$ which are inactive at some stage after σ_1 (and so forever). These will give incorrect answers, i.e. $\{\delta\}^\Delta(x) \neq C(x)$ for some x , while all the others give only correct values of C . Thus if we could bound, say by σ_2 , the stages at which δ 's in B_e become inactive, we could compute C as before by finding for each x the first computation of $\{\delta\}_\sigma^\Delta(x) = C^\sigma(x)$ for any $\sigma > \sigma_2$.

Once again if the set W of $\delta \in B_e$ that becomes inactive were α -finite the desired bound would exist by admissibility. The problem however is that W is only α -r.e. and there can be α -r.e. subsets of α -finite sets (B_e here) which are not α -finite. (This of course was the cause of our first problem — $C \cap N$ might have been α -r.e. but not α -finite.) The solution here too is to make the listing of reduction procedures (as distinct from the priority ordering of blocks of procedures) so short that no bounded α -r.e. subset can be α -finite. Thus we need a short listing of the ordinals less than α but we must also be able to generate it in a recursive way. The key notion here is that of the *projectum*, α^* , of α : α^* is the least β such that there is an α -recursive f mapping α one-one into β . The reason that this idea embodies the solution to our problem is the following:

THEOREM. *Any α -r.e. subset of any $\delta < \alpha^*$ is α -finite.*

(The proof is easy from a recursion theoretic viewpoint: the usual recursive enumeration without repetition of an α -infinite α -r.e. subset of δ would give a map from α into δ .) Thus we need only use an α^* list of our reduction procedures to make W α -finite and solve our last problem.

All that remains is to combine our solutions — we must divide up α^* into γ many blocks. Let $f: \alpha \rightarrow \alpha^*$ be a one-one α -recursive projection and let $h: \gamma \rightarrow \alpha$ be a Σ_2 map unbounded in α . Our blocks are then given by $B_e = fh(e)$ for $e < \gamma$. Note that by admissibility the range of f^{-1} is bounded on any proper initial segment of α^* . Thus $h''\gamma$ projects to an unbounded sequence in α^* and so we include every reduction procedure in these blocks. Moreover, by our previous remarks we can α -recursively approximate these blocks, say by $B_e(\sigma)$, so that for each e , $B_e(\sigma)$ is equal to B_e from some point on. We can also guess at $f^{-1}(\delta)$ for any $\delta < \alpha^*$ in an α -recursive way by the usual procedure (e.g. compute $f(\eta)$ for $\eta < \sigma$ and see if you get δ). Combining the various approximations we can now precisely describe our construction with notational conventions as before.

At stage σ we find for each $e < \gamma$ the least computation of $\{f^{-1}\delta\}_\sigma^\alpha(x) = C^\sigma(x)$ for some e -active $\delta \in B_e(\sigma)$ (x is the least y which is not the argument of some negative e -requirement). We then create a negative e -requirement and proceed with the rest of the construction exactly as above.

The verification that the construction succeeds proceeds as in ordinary recursion theory with the new difficulties handled as we have described. By induction there are only α -finitely many e' -requirements for $e' < e$; thus there is a bound on their creation given by a Σ_2 function. As $e < \gamma$ they form a single α -finite set N and we have a bound σ_0 on the stages at which they are created. By the regularity of C we have a stage $\sigma_1 \geq \sigma_0$ by which all elements of N have been enumerated in C . We can also take σ_1 to be large enough so that $B_e(\sigma)$ and $f^{-1}(\delta)$ for $\delta \in B_e$ have all reached their final values. Once again e -requirements now created are permanent. As $B_e < \alpha^*$ the $\delta \in B_e$ that become inactive form an α -finite set and so contribute only boundedly much. Thus if there were α -infinitely many e -requirements for A we could again compute C α -recursively for our contradiction. Thus there are only α -finitely many e -requirements for A . The B part of the argument is the same and the induction continues.

Finally to see that $C \not\leq_\alpha A$ (or $C \not\leq_\alpha B$) we suppose that $C \leq_\alpha A$ with e' giving the reduction procedure as in the definition of $\leq_\alpha$. Let $f(e') = \delta \in B_e$ for some e . We can now argue (beginning at stage σ_1) that there must be α -infinitely many e -requirements created. By choice of δ there are correct computations of $\{f^{-1}(\delta)\}^\alpha(x) = C(x)$ for every x , so some requirement must be created for each x . As this contradicts our last result, we have that $C \not\leq_\alpha A$ (and similarly $C \not\leq_\alpha B$) as required.

This completes the proof of the Splitting Theorem. (For more details see SHORE [1975a].) We will now see how the ideas used to overcome the special difficulties in α -recursion theory interact with some other areas of research.

4. Interactions and applications

We begin with the notion of projectum which played a key role in our proof and which is closely connected with some of the important set-theoretic concerns about the fine structure of L . An obvious question that arises if one is studying the constructible hierarchy is just when sets are constructed. Thus for example all (constructible) subsets of ω are constructed by level $\aleph_1$ (of L) but one wants to know exactly at which levels

they occur. This particular question was answered by BOLOS and PUTNAM [1968] (who incidentally were working on degree hierarchies in ordinary recursion theory). The results are generalized in KRIPKE [1964a] and PLATEK [1966], while the best (and most general) results are in JENSEN [1972]:

THEOREM. *There is a subset of δ in $L_{\alpha+1} - L_\alpha$ given by a definition which is $\Sigma_n(\Delta_n)$ over L_α iff there is a function $f: \alpha \rightarrow \delta$ which is one-one and Σ_n over L_α (and onto δ).*

For the example of $\delta = \omega$ this says that a new subset of ω is constructed at level α just in case everything becomes countable at that level.

If we consider admissible α with $n = 1$ and apply the appropriate translation, we see that this is precisely the key fact about the projectum α^* of α : If one can't map α one-one into δ by an α -recursive function ($=$ total $\Sigma_1 = \Delta_1$) then there is no new α -r.e. ($= \Sigma_1$) subset of δ (so they are all α -finite). The general result of Jensen plays a key role in both set-theoretic and later recursion-theoretic results.

For work in α -recursion theory it is often necessary to use more complicated projections than just Σ_1 so as to get even shorter listings. As examples we cite the minimal pair constructions of LERMAN and SACKS [1972] and SHORE [1975b] (as well as LEGGETT and SHORE [1976]) in which the Σ_2 projectum is used to list the reduction procedures and requirements. In another vein a relativized version of the theorem for α -r.e. sets and $n = 1$ is used in SHORE [1976a] to show that the α -r.e. degrees are dense. Of course such higher-level projections can be introduced into α -recursive constructions only at the expense of complicating the approximation procedures and weakening the convergence properties needed in the proofs.

The main set-theoretical applications of projecta followed from Jensen's remarkable uniformization theorem:

THEOREM (JENSEN [1972]). *Every Σ_n relation over L_α can be uniformized by a function Σ_n over L_α .*

Although this result obviously has a recursion-theoretic flavor, it was a key ingredient of many of Jensen's purely set-theoretical results. As a prime example we cite the results of JENSEN [1972] that Souslin's hypothesis fails in L . (There are many other results related by their methods of both combinatorial and model-theoretic character.) We should also note that Jensen's proofs of these results have an additional recursion-theoretic

touch. They depend heavily on the idea of uniformity. It is by proceeding always in a prescribed uniform way that the construction is carried past limit stages.

As a final application of these notions we cite the recent work of JOCKUSCH and SIMPSON [1976]. Here the idea of generalized projecta and the related one of coding L_α as a subset of the projectum came back to the source of its original motivation — degree hierarchies in ordinary recursion theory. They are used (together with Sacks' perfect set forcing) to prove results on definability in the theory of Turing degrees with jump. For example, it is shown that the ramified analytic hierarchy is definable level by level in the theory of degrees with jump.

The other major innovation needed for the proof in Section 3 (the blocking technique) has had some repercussions for axiomatic recursion theory. A key question for such an approach is what is needed to do priority arguments, as these are perhaps the deepest and most characteristic methods of ordinary recursion theory. In a typical approach to an axiomatic recursion theory (as in MOSCHOVAKIS [1971]), the main structural loss (relative to α -recursion theory) is the recursive wellordering of the universe. In its place one has only some nice sort of prewellordering. Although this does not seem to be quite enough to do priority arguments (see SIMPSON [1974b] who, however, needs the axiom of determinateness for his counterexample), the blocking technique does supply some answers. One can indeed block all elements of a single level of the prewellordering (assuming they are "finite"), but one still seems to need a notion of projection to argue that each block settles down. Thus one can give an extended axiomatization which allows one to employ this technique to carry out many priority arguments. (This, too, is pointed out in SIMPSON [1974b].)

Finally we would like to mention two applications of the overall results and methods of priority arguments in α -recursion theory. The first is to enable one to do certain forcing constructions over uncountable structures. This idea is used for example in SHORE [1974b] where a priority argument is done on a forcing construction. A special case of the results there shows that over every model of set theory with, say, Σ_n global choice there are Σ_n classes A, B such that neither is Δ_n in the other. Another example of mixing a forcing construction with α -recursion theory appears in SIMPSON [1974a]. There it is used to prove an analog of Friedberg's theorem on the jump operator for α -degrees.

The last application of these methods we consider is to recursion in higher type objects. HARRINGTON [1973] has given a method for directly

translating certain results of α -recursion theory into ones about higher type objects. The only added proviso is that the constructions in α -recursion theory must be uniform in the sense that no infinite parameters are used to describe it. Although we did not bother to do this here (we used both γ and α^*), it can be done. (See SHORE [1975a] and MAASS [1977c] for the Splitting Theorem and SHORE [1974b] for the Friedberg–Muchnick solution to Post’s problem.) Thus we “automatically” have analogs for the priority argument constructions from α -recursion theory in the theory of higher type objects.

5. Bibliographic guide

We have tried to give a complete listing of papers devoted to α -recursion theory with very brief summaries of their contents. As a rule we list abstracts and summarize theses only when we do not know of the material’s having appeared elsewhere. A fair number of papers dealing with α -recursion theory only peripherally or with its connections with other subjects have also been listed but not summarized.

For the reader interested in pursuing α -recursion theory we recommend SACKS [1978] (when available) as a starting point. Until then, SIMPSON [1974a] and SHORE [1975a] are reasonable first papers to read. For more information on and other approaches to priority arguments and the α -r.e. degrees we suggest SACKS and SIMPSON [1972], LERMAN [1972] and (for the committed) SHORE [1976a]. For the lattice of α -r.e. sets one might begin with LERMAN and SIMPSON [1973], followed by LERMAN [1974a] on maximal sets and LERMAN [1975b, 1976] on general lattice-theoretic problems.

There are also a number of important topics that we have not mentioned at all here. The jump operator is considered in SIMPSON [1974a] and in SHORE [1976b]. The phenomena of non-regularity and non-hyperregularity are investigated in SIMPSON [1971] and the structure of such degrees is analyzed in SHORE [1975b].

Turning to a wider ranging view we mention some starting points for work in other areas related to α -recursion theory. For model theory and a general view of admissibility see Chapter A.7 and BARWISE [1975]. Historically more relevant papers include BARWISE [1969] and KARP [1964]. For inductive definitions the basic reference is MOSCHOVAKIS [1974] with the relation to α -recursion theory coming in Chapter 9 which gives the results of BARWISE, GANDY and MOSCHOVAKIS [1971]. For the more intimate connections with admissible ordinals see CENZER [1974]. Axiomatic recursion theory is represented by MOSCHOVAKIS [1971] and FRIEDMAN [1971].

SIMPSON [1974b] is also relevant here. Applications of α -recursion theory to higher type objects are in HARRINGTON [1973] and in LOWENTHAL [1974]. The fine structure of L is best set forth in Chapter B.5 or in JENSEN [1972]. Earlier papers in this area connected with recursion theory include JENSEN and KARP [1971] and GANDY [1974].

Annotated bibliography

ADDISON, J.W., L. HENKIN and A. TARSKI

[1965] *The Theory of Models*, Proceedings of the 1963 International Symposium at Berkeley (North-Holland, Amsterdam).

BAR-HILLEL, Y., editor

[1965] *Logic, Methodology and Philosophy of Science*, Proceedings of the 1964 International Congress (North-Holland, Amsterdam).

BARWISE, J.K.

[1969] Infinitary logic and admissible sets, *J. Symbolic Logic*, **34**, 226–252.

[1975] *Admissible Sets and Structures* (Springer, Berlin).

BARWISE, J.K., R.O. GANDY and Y.N. MOSCHOVAKIS

[1971] The next admissible set, *J. Symbolic Logic*, **36**, 108–120.

BOOLOS, G. and H. PUTNAM

[1968] Degrees of unsolvability of constructible sets of integers, *J. Symbolic Logic*, **33**, 497–513.

CENZER, D.

[1974] Ordinal recursion and inductive definitions, in: FENSTAD and HINMAN [1974] pp. 221–264.

CHONG, C.T.

[1973] Tame Σ_2 functions in α -recursion theory, Thesis, Yale University, New Haven, CT.

[1974] Almost local non- α -recursiveness, *J. Symbolic Logic*, **39**, 552–562.

Studies the question of when, for a non- α -recursive α -r.e. set A , is $A \cap \gamma$ non- γ -recursive for $\gamma < \alpha$.

[1976a] An α -finite injury method of the unbounded type, *J. Symbolic Logic*, **41**, 1–17.

Two theorems: 1. $\forall \alpha$ -r.e. $a \neq 0 \exists \alpha$ -r.e. $b <_\alpha a$ with $b \mid c$ (proof uses $\text{tor}2p$). 2. $\forall \alpha$ -r.e. $a \neq 0 \exists \alpha$ -r.e. $b <_\alpha a$ which is not the glb of two α -r.e. degrees.

[1976b] Minimal upper bounds for ascending sequences of α -recursively enumerable degrees, *J. Symbolic Logic*, **41**, 250–260.

Partial results on subject of title.

CHONG, C.T. and M. LERMAN

[1976] Hyperhypersimple α -r.e. sets, *Ann. Math. Logic*, **9**, 1–48.

Hhs sets defined as ones whose supersets in $\mathcal{E}^*(\alpha)$ form a Boolean algebra. Relation to usual array definition and medley of existence and non-existence results.

CROSSLEY, J.N.

- [1967] *Sets, Models and Recursion Theory*, Proceedings of the Summer School in Mathematical Logic and Tenth Logic Colloquium Leicester, August–September 1965 (North-Holland, Amsterdam).

DRISCOLL, G.C., JR.

- [1965] Contributions to metarecursion theory, Thesis, Cornell University, Ithaca, NY.
 [1968] Metarecursively enumerable sets and their metadegrees, *J. Symbolic Logic*, **33**, 389–411.

Two important results for ω_1^{ck} -recursion theory $\leq_{\omega_1^{\text{ck}}}$ is intransitive and the ω_1^{ck} -r.e. degrees are dense.

FENSTAD, J.E. and P.G. HINMAN

- [1974] *Generalized Recursion Theory*, Proceedings of the 1972 Oslo Symposium (North-Holland, Amsterdam).

FRIEDMAN, H.

- [1971] Axiomatic recursive function theory, in: GANDY and YATES [1971] pp. 113–137.

FUKUYAMA, M.

- [1971] Some concepts of recursiveness on admissible ordinals, *J. Math. Soc. Japan*, **23**, 435–451.

Details of the proofs of equivalences of various definitions of admissible ordinals and recursiveness on them.

GANDY, R.O.

- [1965] Review #4677, *Math. Rev.*, **29**, 882.
 [1974] Set theoretic functions for elementary syntax, in: JECH [1974] pp. 103–126.

GANDY, R.O. and C.M.E. YATES, editors

- [1971] *Logic Colloquium '69*, Proceedings of the Summer School and Colloquium in Mathematical Logic, Manchester, August, 1969 (North-Holland, Amsterdam).

HARRINGTON, L.

- [1973] Contributions to recursion theory in higher types, Thesis, M.I.T., Cambridge, MA.

HIRANO, M.

- [1969] Some definitions for recursive functions of ordinal numbers, *Sci. Rep. Tokoyo Kyoiku Daigaku, Sect A*, **10**, 135–141.

Equivalence of definitions of KRIPKE [1964a] and TUGUÉ [1964].

JECH, T.J., editor

- [1974] *Axiomatic Set Theory*, Proceedings of Symposia in Pure Mathematics, Vol. XIII, part 2 (Am. Math. Soc., Providence, RI). (The UCLA 1967 Set Theory Conference.)

JENSEN, R.B.

- [1972] The fine structure of the constructible hierarchy, *Ann. Math. Logic*, **4**, 229–308.

JENSEN, R.B. and C. KARP

- [1971] Primitive recursive set functions, in: SCOTT [1971] pp. 143–176.

JHU, R.

- [1973] Contributions to axiomatic recursion theory and related aspects of alpha-recursion theory, Thesis, University of Toronto, Toronto, Ont.

Some category (topological sense) results: if $0 <_\alpha B$, then $\{x \mid x \mid B\}$ is meager for countable α .

JOCKUSCH, C.G., JR. and S.G. SIMPSON

- [1976] A degree theoretic definition of the ramified analytical hierarchy, *Ann. Math. Logic*, **1**, 1–32.

KARP, C.

[1964] *Languages with Expressions of Infinite Length* (North-Holland, Amsterdam).

KINO, A. and G. TAKEUTI

[1962] On hierarchies of predicates of ordinal numbers, *J. Math. Soc. Japan*, **14**, 199–232.

(Assume $V = L$.) Defines recursion (on $\aleph_1$) via Kleene type construction of primitive recursive functions and μ operator. Equivalent to TAKEUTI [1960]. Gives basic theorems of recursion theory. Investigates connections with models of set theory and analytical hierarchy (e.g. Δ_n here is usual Δ_{n+1}^1).

KREISEL, G.

[1961] Set theoretic problems suggested by the notion of potential totality, in: *Infinitistic Methods*, Proceedings of the Symposium on Foundations of Mathematics, Warsaw, 2–9 September 1959 (Pergamon Press, Oxford) pp. 103–140.

The beginnings of an approach to ω -models and recursion theory. Π_1^1 is the analog of r.e. and Δ_1^1 is that of finite (first use of a generalization of finiteness in this setting). Used notations for HYP subsets of ω as domain of theory.

[1965] Model theoretic invariants: applications to recursive and hyperarithmetical operations, in: ADDISON et al. [1965] pp. 190–205.

A model theoretic approach to generalized recursion based on notion of rigidly contained structures. Recursion on ω_1^{ck} and ω -logic as an example.

[1967] Relative recursiveness in metarecursion theory (abstracts) *J. Symbolic Logic*, **32**, 442.

Relations between recursion on ω_1^{ck} and (uniform) implicit invariant definitions. See also KUNEN [1968].

[1971] Some reasons for generalizing recursion theory, in: GANDY and YATES [1971] pp. 139–198.

The major paper devoted to the mathematical and philosophical issues of generalizing recursion theory.

KREISEL, G. and G.E. SACKS

[1963] Metarecursive sets I, II (abstracts), *J. Symbolic Logic*, **28**, 304–305.

I. The setting for abstract recursion theory in terms of model theoretic invariants.

II. Recursion theoretic results on ω_1^{ck} , $\exists$ maximal simple ω_1^{ck} -r.e. set and an ω_1^{ck} -incomplete one.

[1965] Metarecursive sets, *J. Symbolic Logic*, **30**, 318–338.

Gives actual proofs for results of above abstracts. Basic introductory paper on metarecursion theory i.e., $\alpha = \omega_1^{ck}$.

KRIPKE, S.

[1964a] Transfinite recursion on admissible ordinals I, II (abstracts), *J. Symbolic Logic*, **29**, 161–162.

I. Gives equation calculus for recursion on ordinals, defines admissibility and notes that basic theorems hold.

II. Cardinals are admissible as are many other ordinals. α -finite is equivalent to being a member of L_α . Admissibility equivalent to satisfying axioms for weak set theory. Notion of projectum. Friedberg–Muchnick theorem for α^* a cardinal.

[1964b] Admissible ordinals and the analytic hierarchy (abstract), *J. Symbolic Logic*, **29**, 162.

Relations between admissible ordinals and analytic hierarchy and ordinals.

[1967] Transfinite recursion, constructible sets and analogs of large cardinals, unpublished lecture notes from UCLA 1967 Conference in Axiomatic Set Theory.

General description and heuristic explanation of recursion theory on ordinals via equation calculus. Describes equivalence to notions in terms of L_α and axioms for a weak set theory. The projectum and the key theorem. Discusses recursive analogs of Mahlo numbers and relations of α -recursion to δ_α^1 , Π_2^1 and Δ_2^1 .

KUNEN, K.

[1968] Implicit definability and infinitary languages, *J. Symbolic Logic*, **33**, 446–451.

LEGGETT, A.

[1973] Maximal α -r.e. sets and their complements, Thesis, Yale University, New Haven, CT.

[1974] Maximal α -r.e. sets and their complements, *Ann. Math. Logic*, **6**, 293–357.

Extends LERMAN [1974a]. Gives necessary and sufficient conditions for the possible order types of complements of maximal sets. Decides extensional equivalence of many alternate definitions of maximal α -r.e. sets

LEGGETT, A. and R.A. SHORE

[1976] Types of simple α -recursively enumerable sets, *J. Symbolic Logic*, **41**, 681–694.

Extension of LERMAN [1975a]. Uses ideas of major subset and hyperhypersimple set to distinguish 1-types of simple α -r.e. sets for all α . Introduces method to use Σ_2 projection in priority arguments when it is less than the $\sigma 2cf(\alpha)$.

LERMAN, M.

[1972] On suborderings of the α -recursively enumerable α -degrees, *Ann. Math. Logic*, **4**, 369–392.

Embeds any α -finite upper-semilattice in the α -degrees. Introduces the important notion of tame Σ_2 projection to give new version of finite injury arguments.

[1973] Admissible ordinals and priority arguments, in: MATHIAS and ROGERS [1973] pp. 311–344.

Gives heuristic description of construction of a minimal pair of r.e. degrees in ordinary and α -recursion theory. Introduces “pinball” metaphor.

[1974a] Maximal α -r.e. sets, *Trans. Am. Math. Soc.*, **188**, 341–386.

Considers various possible definitions of maximal α -r.e. set. Proves they exist (for reasonable definitions) if $s3p(\alpha) = \omega$. Introduces this new ($s3$) projection given by recursive approximation with two extra variables.

[1974b] Least upper bounds for pairs of α -r.e. α -degrees, *J. Symbolic Logic*, **39**, 49–56.

No minimal pair of α -r.e. degrees can have join $0'$.

[1976a] Types of simple α -recursively enumerable sets, *J. Symbolic Logic*, **41**, 419–426.

There are distinct 1-types in $\mathcal{E}(\alpha)$ for simple sets for many α . Uses major subset (every α -r.e. set has one) and hyperhypersimplicity. See also LEGGETT and SHORE [1976].

[1976b] Ideals of generalized finite sets in the lattice of α -recursively enumerable sets, to appear.

$\exists!$ ideal of generalized finite sets definable over $\mathcal{E}(\alpha)$. For these sets $\mathcal{E}(\alpha)$ and $\mathcal{E}^*(\alpha)$ are equidecidable.

[1976c] Congruence relations, filters, ideals and definability in lattices of α -recursively enumerable sets, *J. Symbolic Logic*, **41**, 405–418.

$\exists$ largest ideal, filter and equivalence relation definable in $\mathcal{E}(\alpha)$. Classifies all ideals for some α and leaves only two possibilities for others. In any case there are only finitely many. Points out that main result of MACHTEY [1971] works only for sentences not $\forall\exists$.

LERMAN, M. and G.E. SACKS

[1972] Some minimal pairs of α -recursively enumerable degrees, *Ann. Math. Logic*, **4**, 415–442.

If greatest cardinal of $L_\alpha = \sigma 2p(\alpha) < \tau 2p(\alpha) \leq \alpha$, then there is a minimal pair of α -r.e. degrees. See also SHORE [1976a].

LERMAN, M. and S.G. SIMPSON

[1973] Maximal sets in α -recursion theory, *Israel J. Math.*, **4**, 236–247.

Some necessary and some sufficient conditions for the existence of maximal α -r.e. sets especially the necessity of countability. See also LERMAN [1974a]. Scattered results on r -maximal sets as well.

LEVY, A.

[1963] Transfinite computability, *Notices Am. Math. Soc.*, **10**, 286.

Turing machine definition of recursion on regular cardinals equivalent to TAKEUTI [1960] approach and one similar to MACHOVER [1962].

LOWENTHAL, F.D.

[1973] Some results on measure and category in α -recursion theory, *Notices Am. Math. Soc.*, **20**, A–450.

For countable α : sets above (in $\leq_\alpha$ or $\leq_{\alpha\alpha}$) a given non- α -recursive one have measure 0 and are of 1-st category. Set of all joins of two degrees has measure 1.

[1974] The minimal pair problem for higher type objects, Thesis, M.I.T., Cambridge, MA.

Considers applying methods of HARRINGTON [1973] to minimal pair argument of LERMAN and SACKS [1972] to give results on higher type objects.

MACHOVER, M.

[1961] The theory of transfinite recursion, *Bull. Am. Math. Soc.*, **67**, 575–578.

Introduces an equation calculus for recursion theory on regular cardinals using a sup operator and functions with infinitely many variables. Under assumption that $V = L$ recursively Gödel numbers process and notes analogs of basic recursion theoretic facts. Gives a typical application to infinitary languages. For successor cardinals α the set of satisfiable formulas of $L_{\alpha,\alpha}$ is not α -arithmetical.

[1962] The theory of transfinite recursion (in Hebrew), Thesis, Hebrew University of Jerusalem, Jerusalem.

MACHTEY, M.

[1969] Intrinsic consistency results and lattices of recursively enumerable sets in abstract recursion theory, Thesis, M.I.T., Cambridge, MA.

[1970] Admissible ordinals and intrinsic consistency, *J. Symbolic Logic*, **35**, 389–400.

One cannot in general find an intrinsically consistent (i.e. applicable to all sets) reduction procedure that can replace a given one if α is not a cardinal. One can if α is a cardinal and $V = L$.

[1971] Admissible ordinals and lattices of α -r.e. sets, *Ann. Math. Logic*, **2**, 379–417.

Claims Lachlan's decision procedure for $\forall\exists$ formulas of $\mathcal{E}^*$ works for α when $\alpha^* = \omega$, but see LERMAN [1976c] for a counterexample at the second quantifier level.

[1974] Minimal degrees in generalized recursion theory, *Z. Math. Logik Grundlagen Math.*, **20**, 133–148.

Modifies MACINTYRE [1973] to show that $\exists 2^{\aleph_0}$ minimal α -degrees for countable α . Main result is that for $\alpha^* = \omega$ there is a minimal α -degree below each α -r.e. degree.

MACINTYRE, J.M.

[1968] Contributions to metarecursion theory, Thesis, M.I.T., Cambridge, MA.

In addition to next two items studies subsets of ω generic over $L_{\omega_1^{\text{ck}}}$ and structure of α -degrees below such a set.

[1973] Minimal α -recursion theoretic degrees, *J. Symbolic Logic*, **38**, 18–28.

There exist minimal α -degrees for countable α and regular cardinals of L .

[1974] Non-initial segments of the α -degrees, *J. Symbolic Logic*, **38**, 368–388.

$\forall \alpha < \aleph_1 \exists A \subseteq \alpha$ (every countable distributive lattice with 0 and 1 is isomorphic to an initial segment of α -degrees above A). Thus these theories of α -degrees are undecidable.

MATHIAS, A.R.D. and H. ROGERS, editors

[1973] *Cambridge Summer School in Mathematical Logic*, held in Cambridge/England, August 1–21, 1971 (Springer, Berlin).

METAKIDES, G.

[1972] α -degrees of α -theories, *J. Symbolic Logic*, **37**, 667–682.

For every ω_1^{ck} -r.e. $X \subseteq \omega \exists \omega_1^{\text{ck}}$ -theory, $T(X)$, with bounded ω_1^{ck} -r.e. axioms of same degree as X . $\forall X \subseteq \beta < \omega_1^{\text{ck}} \exists T(X)$ of same degree. Same proof works for all α .

MOSCHOVAKIS, Y.N.

[1971] Axioms for computation theories — first draft in: GANDY and YATES [1971] pp. 199–255.

[1974] *Elementary Induction on Abstract Structures* (North-Holland, Amsterdam).

MYERS, D.L.

[1970] Meta-arithmetical hierarchies, Thesis, M.I.T., Cambridge, MA.

Considers relativization in recursion on ω_1^{ck} and examines possible notions of jump and arithmetical hierarchy with partial results.

OHASHI, K.

[1970] On a question of G.E. Sacks, *J. Symbolic Logic*, **35**, 46–50.

Intrinsically consistent reduction procedures are not sufficient. See also MACHTEY [1970].

OWINGS, J.C., JR.

[1966] Topics in metarecursion theory, Thesis, Cornell University, Ithaca, NY.

[1967] Recursion, metarecursion and inclusion, *J. Symbolic Logic*, **32**, 173–179.

Set A is of type 1 if for every B maximal in A there is a maximal C such that $A \cap C = B$. Otherwise A is of type 2. Maximal ω_1^{ck} -r.e. sets A with $\bar{A}$ unbounded are of type 1 with $\bar{A}$ bounded of type 2. Both exist.

[1969] Π_1^1 -sets, ω -sets and metacompleteness, *J. Symbolic Logic*, **34**, 194–204.

Every ω_1^{ck} -degree of a non-regular ω_1^{ck} -r.e. set or equivalently of a Π_1^1 - Σ_1^1 subset of ω contains such a set with complement of order type ω . Every non-regular ω_1^{ck} -r.e. set has some complete r.e. set weakly recursive in it so $\leq_{\omega_1^{\text{ck}}}$ is intransitive on Π_1^1 sets.

- [1970] The metarecursively enumerable sets but not the Π_1^1 sets can be enumerated without repetitions, *J. Symbolic Logic*, **35**, 223–229.

Proves the theorem of title.

- [1971] A splitting theorem for simple Π_1^1 sets, *J. Symbolic Logic*, **36**, 433–438.

Any simple Π_1^1 set (= simple ω_1^{ck} -r.e. non- ω_1^{ck} -recursive subset of ω) can be split into disjoint Π_1^1 sets of strictly smaller ω_1^{ck} -degrees.

PLATEK, R.

- [1966] Foundations of recursion theory, Thesis, Stanford University, Stanford, CA.

Develops α -recursion theory as a special case of generalized recursion theory. Approach is via definability by (primitive) recursion. Then adds on a search operator. Isolates correct primary notions (admissibility, α -finite, projectum etc.) and establishes basic recursion theoretic facts and the equivalences with the set theoretic approach.

ROGERS, H., JR.

- [1967] *Theory of Recursive Functions and Effective Computability* (McGraw-Hill, New York).

SACKS, G.E.

- [1966a] *Degrees of Unsolvability*, Annals of Mathematics Studies, Vol. 55 (Princeton University Press, Princeton, NJ, 2nd ed.).

- [1966b] Metarecursively enumerable sets and admissible ordinals, *Bull. Am. Math. Soc.*, **72**, 59–64.

Describes meta (= ω_1^{ck}) recursion in terms of Π_1^1 = r.e. and also via equation calculus. $\exists$ two Π_1^1 sets which are ω_1^{ck} -incomparable. Announces results of SACKS [1966c].

- [1966c] Post's problem, admissible ordinals and regularity, *Trans. Am. Math. Soc.*, **124**, 1–23.

Every α -r.e. degree contains a regular α -r.e. set. Uses a weak priority argument to show that $\exists$ (with respect to all reducibilities) an incomplete non- α -recursive α -r.e. set. Introduces notions of regularity and hyperregularity. $\exists$ countable α with no maximal α -r.e. set.

- [1967] Metarecursion theory, in: CROSSLEY [1967] pp. 243–263.

A review and exposition of KREISEL and SACKS [1965] and the basic results of recursion on ω_1^{ck} but using equation calculus in place of notations from $\mathcal{O}$ and Π_1^1 . Also shows that every non-regular ω_1^{ck} -r.e. set is of same ω_1^{ck} -degree as a Π_1^1 subset of ω . Announces results of SACKS [1971].

- [1971] On the reducibility of Π_1^1 sets, *Advances in Mathematics*, **7**, 57–82.

Uses ω_1^{ck} -infinite, coinfinite forcing conditions to build Π_1^1 sets which are ω_1^{ck} -subgeneric (= hyperregular) and incomparable with respect to arbitrary computation of less than ω_1^{ck} steps. Analogous results for $\alpha^* = \omega$.

- [1978] *Higher Recursion Theory* (Springer, Berlin), to appear.

Introduction to α -recursion theory (Chapters V, VI). Includes special case of $\alpha = \omega_1^{ck}$ and some priority arguments for all α . Contains most of the basic facts and definitions.

SACKS, G.E. and S.G. SIMPSON

- [1972] The α -finite injury method, *Ann. Math. Logic*, **4**, 323–367.

First real priority argument for every α to show that $\exists$ hyperregular α -incomparable α -r.e. sets. Argues inside a sequence of Σ_1 substructures of L_ω for most difficult case.

SCOTT, D., editor

- [1971] *Axiomatic Set Theory*, Proceedings of Symposia in Pure Mathematics, Vol. 13, Part 1 (Am. Math. Soc., Providence, RI). (The UCLA 1967 Set Theory Conference.)

SHOENFIELD, J.R.

- [1971] *Degrees of Unsolvability* (North-Holland, Amsterdam).

SHORE, R.A.

- [1972a] Priority arguments in α -recursion theory, Thesis, M.I.T., Cambridge, MA.
[1972b] Minimal α -degrees, *Ann. Math. Logic*, **4**, 393–414.

$\exists$ minimal α (and $c\alpha$) degrees if α is Σ_2 admissible using priority method of SACKS and SIMPSON [1972]. Also for some other ordinals.

- [1974a] Cohesive sets: countable and uncountable, *Proc. Am. Math. Soc.*, **44**, 442–445.

Many uncountable α have cohesive subsets. Which ones do is independent of ZFC.

- [1974b] Σ_n sets which are Δ_n incomparable (uniformly), *J. Symbolic Logic*, **39**, 295–304.

Mixes forcing and priority arguments to show that for each n there are indices $k, l < \omega$ for Σ_n sets which are Δ_n incomparable for every Σ_n admissible α .

- [1975a] Splitting an α -recursively enumerable set, *Trans. Am. Math. Soc.*, **204**, 65–78.

Given non- α -recursive α -r.e. D and a regular α -r.e. C , $\exists A, B$ ($A \cup B = C$, $A \cap B = \emptyset$, $A, B \leq_\alpha C$, $D \not\leq_\alpha A$ and $D \not\leq_\alpha B$). Same theorem for $\leq_{co}$ and usual corollaries for degrees. Introduces blocking technique for priority arguments.

- [1975b] Some more minimal pairs of α -r.e. degrees. *Notices Am. Math. Soc.*, **22**, A524–525.

Settles one of two cases left open in LERMAN and SACKS [1972]: if $\sigma 2cf(\alpha) = \alpha$, then $\exists$ minimal pair of α -r.e. degrees.

- [1975c] The irregular and non-hyperregular α -r.e. degrees, *Israel J. Math.*, **22**, 28–41.

Characterizes ordinals α for which $\exists!$ α -r.e. degree of non-regular or non-hyperregular α -r.e. set. Proves a splitting theorem for such degrees otherwise. $\leq_{wo}$ is intransitive on α -r.e. sets iff there is more than one non-hyperregular α -r.e. degree.

- [1976a] The recursively enumerable α -degrees are dense, *Ann. Math. Logic*, **9**, 123–155.

Extends ideas of SHORE [1975a] to prove density of α -r.e. α - and $c\alpha$ -degrees. First infinite injury priority argument in α -recursion theory.

- [1976b] On the jump of the recursively enumerable α -degrees. *Trans. Am. Math. Soc.*, **217**, 351–363.

Considers various possible definitions for jump operator. Argues for one and shows that there is no incomplete α -r.e. A with $A' = 0''$ if $\exists!$ non-hyperregular α -r.e. degree. There is such an A if $\sigma 2cf(\alpha) = \alpha$. The proof given, that if A is non-hyperregular, $A' \equiv_\alpha 0''$ really only shows that $0'' <_{wo} A'$.

SIMPSON, S.G.

- [1971] Admissible ordinals and recursion theory, Thesis, M.I.T., Cambridge, MA.

In addition to material included in LERMAN and SIMPSON [1973] and SIMPSON [1974a], contains much information on non-hyperregular α -r.e. sets, simple subsets of α^* and many interesting counterexamples.

- [1974a] Degree theory on admissible ordinals, in: FENSTAD and HINMAN [1974] pp. 165–194.

$b >_a 0'$ is regular iff it is the jump of a regular hyperregular degree. Gives necessary and sufficient conditions for the existence of a cone of regular degrees. $\exists$ incomparable α -r.e. a and b such that $(a \vee b)' = 0'$. Gives a survey of other results on α -degrees and considers connections with Jensen's fine structure of L .

[1974b] Post's problem for admissible sets, in: FENSTAD and HINMAN [1974] pp. 437–441.

Using projective determinacy gives an admissible set for which there are no incomparable r.e. sets. Notes that can use blocking technique to give positive answer if have an analog of α^* (calls such sets "thin").

STILLWELL, J.

[1970] Reducibility in generalized recursion theory, Thesis, M.I.T., Cambridge, MA.

Attempts to do priority arguments for all admissible α . The realization that life was not as simple as it here appeared led to the actual solution in SACKS and SIMPSON [1972].

SUKONICK, J.

[1969] Lower bounds for pairs of metarecursively enumerable degrees, Thesis, M.I.T., Cambridge, MA.

There exists a minimal pair of ω_1^{ck} -r.e. degrees.

TAKAHASHI, M.

[1968] Recursive functions of ordinal numbers and Levy's hierarchy, *Comment. Math. Univ. St. Paul*, **17**, 21–29.

Recursive on ON equals Δ_1 if $V = L$.

TAKEUTI, G.

[1954] Construction of the set theory from the theory of ordinal numbers, *J. Math. Soc. Japan*, **6**, 196–220.

[1957] On the theory of ordinal numbers, *J. Math. Soc. Japan*, **9**, 93–113.

[1960] On the recursive functions of ordinal numbers, *J. Math. Soc. Japan*, **12**, 119–128.

Introduces recursion on the ordinals by generating the semi-recursive functions from basic ones via recursion and a minimum operator. Recursive ones are gotten when min is only applied when bounded or total. The main result is that cardinals (in particular singular cardinals) are closed under recursive functions (induction on complexity). Uses theory to show that axioms of TAKEUTI [1957] can be effectivized. Motivation for this is in TAKEUTI [1954].

[1965a] A formalization of the theory of ordinal numbers, *J. Symbolic Logic*, **30**, 295–317.

Results from a paper given at the Symposium of Foundations of Mathematics, Katada, Japan, in October 1962. Presents recursion on ordinals and gives an "effective" consistency proof for set theory by showing that there is a recursive predicate isomorphic to $\in$ on L .

[1965b] Recursive functions and arithmetic functions of ordinal numbers, in: BAR-HILLEL [1965] pp. 179–196.

Considers some axioms of infinity based on a notion of arithmetic inaccessibility.

TUGUÉ, T.

[1964] On the partial recursive functions of ordinal numbers, *J. Math. Soc. Japan*, **16**, 1–31.

Gives an equation calculus for recursion on regular cardinals using sup operator. Shows it equivalent to Takeuti's systems and proves some basic facts like recursion and hierarchy theorems.

Supplement to bibliography*

CHONG, C.T.

[1977] Σ_n -cofinalities in L_α , to appear.

Some results on the possible values of $\sigma ncf(\alpha)$ and its relation to $\delta np(\alpha)$.

FRIEDMAN, S.

[1976] Recursion on inadmissible ordinals, Thesis, M.I.T., Cambridge, MA.

The first work on recursion theory on inadmissible ordinals. Basic facts and definitions. Simple sets exist. A solution to Post's problem for many inadmissible β .

JACOBS, B.E.

[1975] α -computational complexity, Thesis, Courant Institute of Mathematical Sciences, New York University, New York.

[1977a] On generalized computational complexity, *J. Symbolic Logic*, to appear.

Generalizes the basic notions of abstract complexity theory to α -recursion theory. Analogs of compression and gap theorems.

[1977b] The α -union theorem and generalized primitive recursion, to appear.

Proves analog of union theorem and considers two analogs of primitive recursion on admissible α .

[1977c] α -naming and α -speedup theorems, to appear.

Proves analogs of these theorems.

LERMAN, M.

[1977] On elementary theories of some lattices of α -recursively enumerable sets, to appear.

Decides the $\forall\exists$ theory of $\mathcal{E}^*(\alpha)$ for two different classes of ordinals. If $\sigma 2cf(\alpha) = \sigma 2p(\alpha) = \omega$ and $\alpha^* = \alpha$, the theory is that of $\mathcal{E}^*(\omega)$. If $s3cf(\alpha) = \sigma 3p(\alpha) = \alpha$ (e.g. a regular cardinal of L), then a different decidable $\forall\exists$ theory is given.

MAASS, W.

[1977a] Inadmissibility, tame r.e. sets and the admissible collaps, to appear.

Introduces the notion of admissible collaps and studies it and other items in inadmissible recursion theory.

[1977b] On minimal pairs and minimal degrees in higher recursion theory, to appear.

Constructs hyperregular minimal α -r.e. pairs for many α . Applies methods of MAASS [1977a] to construct minimal degrees when $\sigma 2cf(\alpha) = \sigma 2p(\alpha) < \alpha$.

[1977c] The uniform regular set theorem in α -recursion theory, to appear.

Settles a question from SACKS [1966c] by giving a uniform construction of a regular α -r.e. set of the same α -degree as any given α -r.e. set.

SHORE, R.A.

[1976c] Combining the density and splitting theorems for α -r.e. degrees, *Notices Am. Math. Soc.*, **23**, A-598.

If $A' \equiv_\alpha 0'$ and $A <_\alpha D$ are α -r.e., then $\exists B, C$ α -r.e. with $A <_\alpha B$, $C <_\alpha D$ and $B \vee C \equiv_\alpha D$. By SHORE [1976b] there are α (e.g. $\aleph_\alpha^L$) for which $A' \equiv_\alpha 0'$ for every incomplete α -r.e. A . Thus by a result of Lachlan the elementary theories of the α -r.e. degrees with $\leq_\alpha$ are different for $\alpha = \omega$ and $\alpha = \aleph_\omega^L$.

*Recursion in Higher Types**

ALEXANDER S. KECHRIS

YIANNIS N. MOSCHOVAKIS

Contents

Introduction	682
FUNCTIONAL INDUCTION	
1. Monotone operators on partial functions	682
2. Suitable classes of functionals	683
3. The basic constructions	687
4. Relations with ordinary recursion theory	691
5. Recursion in type 2 objects and quantifiers	692
6. The Stage Comparison Theorem	696
7. Semirecursive relations	700
8. The Enumeration Theorem	701
9. Consequences of enumeration	705
RECURSION IN HIGHER TYPES	
10. The type structure over ω	707
11. Kleene classes of functionals on T^*	709
12. Kleene recursion relative to objects of higher type and quantifiers	711
13. Normality and enumeration in higher type recursion	714
14. The original definition of Kleene	716
15. Equivalence of the original Kleene definition with ours	718
16. The Substitution Theorems of Kleene	722
17. Sections and envelopes	728
18. Inductive analysis of semirecursive sets	730
19. Closure under higher existential quantification	733
20. A guide to the literature	734
References	736

* During the preparation of this paper the authors were partially supported by NSF Grants MPS 75-07562 and MPS 74-06732 resp.

Introduction

Recursion in higher types was introduced by KLEENE [1959, 1963] and was soon recognized as a deep and significant extension of the theory of recursive functions on the integers. Our purpose here is to give an exposition of the basic notions and facts of this theory in a manner which will make them accessible to the mathematician with a working knowledge of ordinary recursion theory.

From its inception, higher-type recursion has been considered difficult and somewhat esoteric. Although it has been brought to a seasoned maturity with the contributions of many researchers in the last fifteen years, it has not been understood by as wide a circle of mathematicians as it deserves. This is partly due to the technical difficulty of the basic papers on the subject. More than that, the basic notions of the theory have been considered difficult to understand and foundationally problematical.

Here we will develop higher-type recursion in the context of the general theory of inductive definability. KLEENE [1963] himself saw this possibility and discussed it at the end of Section 10. Later, PLATEK [1966] gave a very satisfactory foundation for the subject within a theory of induction. His work, however, was also technically difficult and not easily applicable to Kleene recursion.

The present approach is due to Moschovakis. A discussion of how it fits within a general theory of induction is given in MOSCHOVAKIS [1976], but knowledge of that paper is not needed to read this one.

We should emphasize that this is an exposition of the elementary parts of the theory of higher-type recursion. In the last section we will make some suggestions on what to read next, for the reader who wants to become an expert.

FUNCTIONAL INDUCTION

1. Monotone operators on partial functions

Fix an infinite set A such that $\omega = \{0, 1, 2, \dots\} \subseteq A$. An n -ary *partial function* (on A , into ω) is any mapping from a subset of A^n into ω . We collect these into a set,

$$\mathcal{P}\mathcal{F}_n(A) = \mathcal{P}\mathcal{F}_n = \{f: f \text{ is an } n\text{-ary partial function}\}.$$

An operator $\Theta : \mathcal{P}\mathcal{I}_n \rightarrow \mathcal{P}\mathcal{I}_n$ is *monotone* if for all $f, g \in \mathcal{P}\mathcal{I}_n$,

$$f \subseteq g \Rightarrow \Theta(f) \subseteq \Theta(g).$$

Each such monotone operator determines a transfinite sequence $\{f_\Theta^\xi\}$ of partial functions by the recursion

$$f_\Theta^\xi = \Theta(f_\Theta^{<\xi}),$$

where $f_\Theta^{<\xi} = \bigcup_{\eta < \xi} f_\Theta^\eta$, i.e.

$$f_\Theta^{<\xi}(\bar{x}) = w \Leftrightarrow \text{for some } \eta < \xi, f_\Theta^\eta(\bar{x}) = w.$$

In particular, $f_\Theta^0 = \Theta(\emptyset)$, where $\emptyset$ is the empty n -ary partial function.

A simple induction shows that

$$\zeta \leq \xi \Rightarrow f_\Theta^\zeta \subseteq f_\Theta^\xi,$$

so by a cardinality argument there is a least ordinal κ such that

$$f_\Theta^\kappa = f_\Theta^{<\kappa} = \bigcup_\xi f_\Theta^\xi.$$

We call f_Θ^κ the partial function *inductively defined* by Θ and we denote it by

$$f_\Theta^\infty = \bigcup_\xi f_\Theta^\xi.$$

It is easy to check that f_Θ^∞ is also the least *fixed point* of Θ , i.e.,

$$\Theta(f_\Theta^\infty) = f_\Theta^\infty \quad \text{and} \quad \Theta(f) \subseteq f \Rightarrow f_\Theta^\infty \subseteq f.$$

2. Suitable classes of functionals

2.1. A *functional* (on A with values in ω) is a partial mapping

$$\Phi : A^n \times \mathcal{P}\mathcal{I}_{k_1} \times \cdots \times \mathcal{P}\mathcal{I}_{k_m} \rightarrow \omega$$

from a Cartesian product of copies of A and some of the spaces $\mathcal{P}\mathcal{I}_k$ into ω , which is *monotone*, i.e.

$$f_1 \subseteq g_1, \dots, f_m \subseteq g_m,$$

$$\Phi(\bar{x}, f_1, \dots, f_m) = w \Rightarrow \Phi(\bar{x}, g_1, \dots, g_m) = w.$$

We allow here that n or m may be 0 — in particular all partial functions are functionals.

The *signature* of the functional

$$\Phi(\bar{x}, \bar{f}) = \Phi(x_1 \cdots x_n, f_1 \cdots f_m)$$

is $(n, k_1 \cdots k_m)$ if f_i is k_i -ary. There is a natural 1-1 correspondence between functionals of signature $(n, k_1 \cdots k_m)$ and monotone operators $\Theta : \mathcal{P}\mathcal{I}_{k_1} \times \cdots \times \mathcal{P}\mathcal{I}_{k_m} \rightarrow \mathcal{P}\mathcal{I}_n$, which associates with $\Phi(\bar{x}, f_1 \cdots f_m)$ the mapping

$$\Theta(f_1 \cdots f_m) = \lambda \bar{x} \Phi(\bar{x}, f_1 \cdots f_m)$$

and to each $\Theta(f_1 \cdots f_m)$ the functional

$$\Phi(\bar{x}, f_1 \cdots f_m) = \Theta(f_1 \cdots f_m)(\bar{x}).$$

In particular, if Φ has signature (n, n) , then the associated Θ is a monotone operator on $\mathcal{P}\mathcal{I}_n$. It will be convenient to abbreviate the ξ -th iterate of Θ by Φ^ξ , so that

$$\Phi^\xi(\bar{x}) = \Phi(\bar{x}, \Phi^{<\xi})$$

with $\Phi^{<\xi} = \bigcup_{\eta < \xi} \Phi^\eta$. We also let $\Phi^\infty = \bigcup_\xi \Phi^\xi$ be the *least fixed point* of (the operator associated with) Φ or the *partial function inductively defined* by Φ .

This definition *relativizes* directly to any finite sequence of partial functions: given $\Phi(\bar{x}, f, \bar{g})$ of signature $(n, n, k_1, \dots, k_m)$, put

$$\Phi^\xi(\bar{x}, \bar{g}) = \Phi(\bar{x}, \lambda \bar{x}' \Phi^{<\xi}(\bar{x}', \bar{g}), \bar{g}),$$

$$\Phi^\infty(\bar{x}, \bar{g}) = w \Leftrightarrow \exists \xi \Phi^\xi(\bar{x}, \bar{g}) = w,$$

where naturally

$$\Phi^{<\xi}(\bar{x}, \bar{g}) = w \Leftrightarrow \exists \eta < \xi \Phi^\eta(\bar{x}, \bar{g}) = w.$$

We call such functionals $\Phi(\bar{x}, f, \bar{g})$ of signature $(n, n, k_1, \dots, k_m)$ *operative* and we call $\Phi^\infty(\bar{x}, \bar{g})$ the functional *inductively defined* by Φ . It has the following minimality property: if $\Psi(\bar{x}, \bar{g})$ satisfies

$$\lambda \bar{x} \Phi(\bar{x}, \lambda \bar{x}' \Psi(\bar{x}', \bar{g}), \bar{g}) \subseteq \lambda \bar{x} \Psi(\bar{x}, \bar{g})$$

for every $\bar{g}$, then $\Phi^\infty \subseteq \Psi$.

2.2. Let $\mathcal{I}$ be a class of functionals on A . The $\mathcal{I}$ -fixed points are all the functionals $\Phi^\infty(\bar{x}, \bar{g})$ which are inductively defined by operative functionals $\Phi(\bar{x}, f, \bar{g})$ in $\mathcal{I}$. We say that $\Psi(\bar{x}, \bar{g})$ is $\mathcal{I}$ -recursive if there is an $\mathcal{I}$ -fixed point $\Phi^\infty(\bar{u}, \bar{x}, \bar{g})$ and a finite sequence of constants $\bar{n} = (n_1 \cdots n_k)$ from ω such that $\Psi(\bar{x}, \bar{g}) = \Phi^\infty(\bar{n}, \bar{x}, \bar{g})$. In particular, a partial function $\varphi(\bar{x})$ is $\mathcal{I}$ -recursive if there is an operative functional $\Phi(\bar{u}, \bar{x}, f)$ in $\mathcal{I}$ and constants $\bar{n}$ from ω such that

$$\varphi(\bar{x}) = \Phi^\infty(\bar{n}, \bar{x}).$$

Our main aim here is to study these $\mathcal{F}$ -recursive partial functions, for various $\mathcal{F}$'s. In order to obtain an interesting theory of $\mathcal{F}$ -recursion, we must impose some minimal closure conditions on the class $\mathcal{F}$.

2.3. DEFINITION. A class of functionals $\mathcal{F}$ is *suitable* if $\mathcal{F}$ contains the initial partial functions and functionals (i)–(v) and is closed under the rules (vi)–(x) below:

(i) *Characteristic function on ω* :

$$\varphi(a) = \chi_{\omega}(a) = \begin{cases} 0 & \text{if } a \in \omega, \\ 1 & \text{if } a \notin \omega. \end{cases}$$

(ii) *Identity on ω* :

$$\varphi(a) = \begin{cases} a & \text{if } a \in \omega, \\ 0 & \text{if } a \notin \omega. \end{cases}$$

(iii) *Successor function*:

$$\varphi(a) = \begin{cases} a + 1 & \text{if } a \in \omega, \\ 0 & \text{if } a \notin \omega. \end{cases}$$

(iv) *Characteristic function of equality on ω* :

$$\varphi(a, b) = \begin{cases} 0 & \text{if } a = b \in \omega, \\ 1 & \text{if } a \neq b \text{ and } a, b \in \omega, \\ 0 & \text{otherwise.} \end{cases}$$

(v) *Evaluation*:

$$\Phi(\bar{x}, f) = f(\bar{x}).$$

It is understood here that Φ is of signature (n, n) , so that $f(\bar{x})$ makes sense. We will omit such trivial side conditions in the sequel.

(vi) *Addition of variables*: if $\Phi(\bar{x}, \bar{f})$ is in $\mathcal{F}$, so is

$$\Psi(\bar{z}, \bar{x}, \bar{y}, \bar{h}, \bar{f}, \bar{g}) = \Phi(\bar{x}, \bar{f}).$$

(vii) *Composition*: if $\Phi(a, \bar{x}, \bar{f})$ and $X(\bar{x}, \bar{f})$ are in $\mathcal{F}$, so is

$$\Psi(\bar{x}, \bar{f}) = \Phi(X(\bar{x}, \bar{f}), \bar{x}, \bar{f}).$$

(viii) *Definition by cases*: if $\Phi(\bar{x}, \bar{f})$ and $X(\bar{x}, \bar{f})$ are in $\mathcal{F}$, so is

$$\Psi(a, \bar{x}, \bar{f}) = \begin{cases} \Phi(\bar{x}, \bar{f}) & \text{if } a = 0, \\ X(\bar{x}, \bar{f}) & \text{if } a \neq 0 \text{ and } a \in \omega, \\ 0 & \text{if } a \notin \omega. \end{cases}$$

(ix) *Substitution of projection*: a *projection* is any mapping of the form

$$\pi(x_1 \cdots x_n) = x_i,$$

where $1 \leq i \leq n$. Thus (ix) asserts that if $\Phi(y_1 \cdots y_m, \bar{f})$ is in $\mathcal{J}$ and $\pi_1 \cdots \pi_m$ are projections, then

$$\Psi(\bar{x}, \bar{f}) = \Phi(\pi_1(\bar{x}) \cdots \pi_m(\bar{x}), \bar{f})$$

is also in $\mathcal{J}$.

(x) *Functional substitutions*: if $\Phi(\bar{x}, g_1 \cdots g_m)$ is in $\mathcal{J}$ and $X_1 \cdots X_m$ are in $\mathcal{J}$ so is

$$\Psi(\bar{x}, \bar{f}) = \Phi(\bar{x}, \lambda \bar{y}_1 X_1(\bar{y}_1, \bar{x}, \bar{f}), \dots, \lambda \bar{y}_m X_m(\bar{y}_m, \bar{x}, \bar{f})).$$

We will use trivial consequences of these closure properties without explicit justification. For example, from (vii) and (viii) it follows that if Φ_0, Φ_1, X are in $\mathcal{J}$, then so is

$$\Psi(\bar{x}, \bar{f}) = \begin{cases} \Phi_0(\bar{x}, \bar{f}) & \text{if } X(\bar{x}, \bar{f}) = 0, \\ \Phi_1(\bar{x}, \bar{f}) & \text{if } X(\bar{x}, \bar{f}) \neq 0, \end{cases}$$

where $X(\bar{x}, \bar{f}) \neq 0$ abbreviates the statement

$$X(\bar{x}, \bar{f}) \text{ is defined and has value } \neq 0.$$

Also from (v), (vi), (ix) and (x) it follows that if $\Phi(x_1 \cdots x_n, f_1 \cdots f_m) \in \mathcal{J}$ and π, ρ are permutations of $\{1, \dots, n\}, \{1, \dots, m\}$ respectively, then

$$\Psi(x_1 \cdots x_n, f_1 \cdots f_m) = \Phi(x_{\pi(1)} \cdots x_{\pi(n)}, f_{\rho(1)} \cdots f_{\rho(m)})$$

is also in $\mathcal{J}$. Finally since $f = \lambda \bar{x} f(\bar{x})$, (v), (ix) and (x) imply that if $\Phi(\bar{x}, g_1, g_2, g_3)$ is in $\mathcal{J}$, then so is

$$\Psi(\bar{x}, f, g) = \Phi(\bar{x}, f, f, \lambda y g(y, \bar{x}, y)).$$

2.4. We will now give two examples of nontrivial functionals which are $\mathcal{J}$ -recursive for any suitable $\mathcal{J}$.

Minimalization. Let

$$\Phi_\mu(\bar{x}, f) = \mu i (f(i, \bar{x}) = 0)$$

$$= \text{the least } i \in \omega \text{ (if one exists) such that } f(i, \bar{x}) = 0$$

$$\text{and for all } j < i, f(j, \bar{x}) \text{ is defined and } f(j, \bar{x}) \neq 0.$$

To see that Φ_μ is $\mathcal{J}$ -recursive, let

$$\Psi(a, \bar{x}, g, f) = \begin{cases} f(a, \bar{x}) & \text{if } f(a, \bar{x}) = 0, \\ g(a + 1, \bar{x}) + 1 & \text{if } f(a, \bar{x}) \neq 0. \end{cases}$$

Clearly $\Psi \in \mathcal{J}$ and it is easy to verify that $\Phi_\mu(\bar{x}, f) = \Psi^\infty(0, \bar{x}, f)$, so that Φ_μ is $\mathcal{J}$ -recursive.

Primitive recursion. Consider the functional $\Phi_p(a, \bar{x}, f_1, f_2)$ defined by

$$\Phi_p(a, \bar{x}, f_1, f_2) = 0 \quad \text{if } a \notin \omega,$$

$$\Phi_p(0, \bar{x}, f_1, f_2) = f_1(\bar{x}),$$

$$\Phi_p(i + 1, \bar{x}, f_1, f_2) = f_2(\Phi_p(i, \bar{x}, f_1, f_2), i, \bar{x})$$

and assume that $\mathcal{J}$ is a suitable class which contains the *predecessor function*

$$a \div 1 = \begin{cases} a - 1 & \text{if } a \in \omega, a \geq 1, \\ 0 & \text{if } a \notin \omega \text{ or } a = 0. \end{cases}$$

Put

$$\Psi(a, \bar{x}, g, f_1, f_2) = \begin{cases} f_1(\bar{x}) & \text{if } a = 0, \\ f_2(g(a \div 1, \bar{x}), a, \bar{x}) & \text{if } a \in \omega, a \neq 0, \\ 0 & \text{if } a \notin \omega. \end{cases}$$

Then $\Psi \in \mathcal{J}$ and it is easy to check that $\Phi_p = \Psi^\infty$, so that Φ_p is $\mathcal{J}$ -recursive. We will see in the next section that we do not really need to assume that $a \div 1$ is in $\mathcal{J}$.

2.5. Let $\mathcal{J}_0 = \mathcal{J}_0(A)$ be the smallest suitable class of functionals on A . More generally, if $\bar{\Phi} = (\Phi_1 \cdots \Phi_n)$ is a finite sequence of functionals, let

$$\mathcal{J}_0[\bar{\Phi}]$$

be the smallest suitable class of functionals containing $\Phi_1 \cdots \Phi_n$. We will usually call the $\mathcal{J}_0[\bar{\Phi}]$ -recursive functionals simply *recursive in $\bar{\Phi}$* .

3. The basic constructions

Our basic tool for constructing complicated inductions is the following.

3.1. SIMULTANEOUS INDUCTION LEMMA. *Let $\mathcal{J}$ be a suitable class of functionals on A , let $\Phi_0(\bar{x}, f_1, f_2, \bar{g})$, $\Phi_1(\bar{y}, f_1, f_2, \bar{g})$ be two functionals in $\mathcal{J}$ and define inductively*

$$\Psi_0^\xi(\bar{x}, \bar{g}) = \Phi_0(\bar{x}, \lambda \bar{x}' \Psi_0^{<\xi}(\bar{x}', \bar{g}), \lambda \bar{y}' \Psi_1^{<\xi}(\bar{y}', \bar{g}), \bar{g}),$$

$$\Psi_1^\xi(\bar{y}, \bar{g}) = \Phi_1(\bar{y}, \lambda \bar{x}' \Psi_0^{<\xi}(\bar{x}', \bar{g}), \lambda \bar{y}' \Psi_1^{<\xi}(\bar{y}', \bar{g}), \bar{g}).$$

Then $\Psi_0^\infty, \Psi_1^\infty$ are both $\mathcal{J}$ -recursive.

PROOF. Let $\bar{0}$ be a sequence of 0's of the appropriate length so that the expressions below make sense and similarly for $\bar{1}$. Put

$$X(a, \bar{x}, \bar{y}, \bar{f}, \bar{g}) = \begin{cases} \Phi_0(\bar{x}, \lambda \bar{x}' f(0, \bar{x}', \bar{0}), \lambda \bar{y}' f(1, \bar{1}, \bar{y}'), \bar{g}) & \text{if } a = 0, \\ \Phi_1(\bar{y}, \lambda \bar{x}' f(0, \bar{x}', \bar{0}), \lambda \bar{y}' f(1, \bar{1}, \bar{y}'), \bar{g}) & \text{if } a \in \omega, a \neq 0, \\ 0 & \text{if } a \notin \omega. \end{cases}$$

Then $X \in \mathcal{J}$ and a trivial induction on ξ shows that

$$\Psi_0^\xi(\bar{x}, \bar{g}) = X^\xi(0, \bar{x}, \bar{0}, \bar{g}), \quad \Psi_1^\xi(\bar{y}, \bar{g}) = X^\xi(1, \bar{1}, \bar{y}, \bar{g}),$$

so that $\Psi_0^\infty, \Psi_1^\infty$ are $\mathcal{J}$ -recursive. (Strictly speaking we have $\Psi_0^\infty(\bar{x}, \bar{g}) = X^\infty(0, \bar{x}, \bar{0}, \bar{g})$, which is not exactly of the right form but it is immediate that

$$\Psi_0^\infty(\bar{x}, \bar{g}) = \tilde{X}^\infty(0, \bar{0}, \bar{x}, \bar{g}),$$

where $\tilde{X}(a, \bar{x}, \bar{y}, \bar{f}, \bar{g}) = X(a, \bar{y}, \bar{x}, \lambda a' \bar{y}' \bar{x}' f(a', \bar{y}', \bar{x}'), \bar{g})$.) $\square$

As an immediate corollary of the preceding result we have the important:

3.2. FUNCTIONAL SUBSTITUTION THEOREM. *Let $\mathcal{J}$ be a suitable class of functionals on A . Then the class of $\mathcal{J}$ -recursive functionals is closed under functional substitutions, i.e., if $\Phi(\bar{x}, g_1 \cdots g_m), X_1 \cdots X_m$ are all $\mathcal{J}$ -recursive so is*

$$\Psi(\bar{x}, \bar{f}) = \Phi(\bar{x}, \lambda \bar{y}_1 X_1(\bar{y}_1, \bar{x}, \bar{f}), \dots, \lambda \bar{y}_m X_m(\bar{y}_m, \bar{x}, \bar{f})).$$

PROOF. Take $m = 1$ for simplicity and consider $\Phi(\bar{x}, g), X(\bar{y}, \bar{x}, \bar{f})$. There are functionals $\Phi_0(\bar{u}, \bar{y}, \bar{x}, h, \bar{f}), \Phi_1(\bar{v}, \bar{x}, h', g)$ in $\mathcal{J}$ such that for some $\bar{n}, \bar{m}$,

$$X(\bar{y}, \bar{x}, \bar{f}) = \Phi_0^\infty(\bar{n}, \bar{y}, \bar{x}, \bar{f}), \quad \Phi(\bar{x}, g) = \Phi_1^\infty(\bar{m}, \bar{x}, g).$$

Consider then the simultaneous induction

$$\Psi_0^\xi(\bar{u}, \bar{y}, \bar{x}, \bar{f}) = \Phi_0(\bar{u}, \bar{y}, \bar{x}, \lambda \bar{u}' \bar{y}' \bar{x}' \Psi_0^{<\xi}(\bar{u}', \bar{y}', \bar{x}', \bar{f}), \bar{f})$$

$$\Psi_1^\xi(\bar{v}, \bar{x}, \bar{f}) = \Phi_1(\bar{v}, \bar{x}, \lambda \bar{v}' \bar{x}' \Psi_1^{<\xi}(\bar{v}', \bar{x}', \bar{f}), \lambda \bar{y}' \Psi_0^{<\xi}(\bar{n}, \bar{y}', \bar{x}, \bar{f})).$$

By the Simultaneous Induction Lemma $\Psi_1^\infty(\bar{v}, \bar{x}, \bar{f})$ is $\mathcal{J}$ -recursive. We claim now that

$$(*) \quad \Psi(\bar{x}, \bar{f}) = \Psi_1^\infty(\bar{m}, \bar{x}, \bar{f}),$$

which completes the proof. To see that $(*)$ holds, check first that $\Psi_0^\xi = \Phi_0^\xi$, for all ξ . From this an easy induction on ξ , using the monotonicity of the functionals in their function arguments, shows that (for each $\bar{f}$)

$$\lambda \bar{v} \bar{x} \Psi_1^\xi(\bar{v}, \bar{x}, \bar{f}) \subseteq \lambda \bar{v} \bar{x} \Phi_1^\infty(\bar{v}, \bar{x}, \lambda \bar{y} X(\bar{y}, \bar{x}, \bar{f})),$$

so that

$$\lambda \bar{x} \Psi_1^\infty(\bar{m}, \bar{x}, \bar{f}) \subseteq \lambda \bar{x} \Psi(\bar{x}, \bar{f}).$$

For the other direction we prove by induction on ξ and using monotonicity again that

$$\lambda \bar{v} \bar{x} \Phi_1^\xi(\bar{v}, \bar{x}, \lambda \bar{y} \Phi_0^{\leq \xi}(\bar{n}, \bar{y}, \bar{x}, \bar{f})) \subseteq \lambda \bar{v} \bar{x} \Psi_1^\xi(\bar{v}, \bar{x}, \bar{f})$$

so that

$$\lambda \bar{v} \bar{x} \Phi_1^\infty(\bar{v}, \bar{x}, \lambda \bar{y} X(\bar{y}, \bar{x}, \bar{f})) \subseteq \lambda \bar{v} \bar{x} \Psi_1^\infty(\bar{v}, \bar{x}, \bar{f}),$$

thus

$$\lambda \bar{x} \Psi(\bar{x}, \bar{f}) \subseteq \lambda \bar{x} \Psi_1^\infty(\bar{m}, \bar{x}, \bar{f})$$

and we are done. $\square$

This result takes a particularly simple form when we substitute a partial function: if $\Phi(\bar{x}, g, \bar{f})$ and φ are $\mathcal{J}$ -recursive, then so is $\Psi(\bar{x}, \bar{f}) = \Phi(\bar{x}, \varphi, \bar{f})$.

Using the Functional Substitution Theorem and the trivial fact that every functional in $\mathcal{J}$ is also $\mathcal{J}$ -recursive, we can immediately see that the class of $\mathcal{J}$ -recursive functionals has all the closure properties of $\mathcal{J}$, so in particular it too is a suitable class. For example, to prove that it is closed under composition consider the functional

$$\Phi_C(\bar{x}, f_1, f_2) = f_2(f_1(\bar{x}), \bar{x}).$$

Clearly $\Phi_C \in \mathcal{J}$ by 2.3(v), (vii). So if $\Phi(a, \bar{x}, \bar{f})$, $X(\bar{x}, \bar{f})$ are $\mathcal{J}$ -recursive, it follows from the Functional Substitution Theorem that

$$\begin{aligned} \Psi(\bar{x}, \bar{f}) &= \Phi(X(\bar{x}, \bar{f}), \bar{x}, \bar{f}) \\ &= \Phi_C(\bar{x}, \lambda \bar{x}' X(\bar{x}', \bar{f}), \lambda a \bar{x}' \Phi(a, \bar{x}', \bar{f})) \end{aligned}$$

is also $\mathcal{J}$ -recursive. Similarly, using 2.4, the class of $\mathcal{J}$ -recursive functionals is closed under minimalization and primitive recursion, at least when $a \div 1$ is in $\mathcal{J}$.

Our last result in this section is probably the most important closure property of the class of $\mathcal{J}$ -recursive functionals, for suitable $\mathcal{J}$. It allows us to use freely $\mathcal{J}$ -recursive functionals in constructing complicated induc-

tions and will be used repeatedly in the sequel. It is also called the *First Recursion Theorem* for functional induction.

3.3. THE INDUCTION COMPLETENESS THEOREM (MOSCHOVAKIS [1976]). *Let $\mathcal{J}$ be a suitable class of functionals on A . If $\Phi(\bar{x}, g, \bar{f})$ is an operative $\mathcal{J}$ -recursive functional, then the fixed point $\Phi^\infty(\bar{x}, \bar{f})$ is also $\mathcal{J}$ -recursive.*

PROOF. Let $\Phi(\bar{x}, g, \bar{f}) = \Psi^\infty(\bar{n}, \bar{x}, g, \bar{f})$, where $\Psi(\bar{u}, \bar{x}, h, g, \bar{f}) \in \mathcal{J}$ and $\bar{n}$ is a sequence of constants. Put

$$X(\bar{u}, \bar{x}, h, \bar{f}) = \Psi(\bar{u}, \bar{x}, h, \lambda \bar{x}' h(\bar{n}, \bar{x}'), \bar{f});$$

clearly $X \in \mathcal{J}$. We claim that

$$(**) \quad \Phi^\infty(\bar{x}, \bar{f}) = X^\infty(\bar{n}, \bar{x}, \bar{f}),$$

which will complete the proof.

To prove (**), show first by an easy transfinite induction on ξ (using monotonicity) that

$$X^\xi(\bar{u}, \bar{x}, \bar{f}) = w \Rightarrow \Psi^\xi(\bar{u}, \bar{x}, \lambda \bar{x}' \Phi^{<\xi}(\bar{x}', \bar{f}), \bar{f}) = w,$$

thus

$$\begin{aligned} \lambda \bar{x} X^\infty(\bar{n}, \bar{x}, \bar{f}) &\subseteq \lambda \bar{x} \Psi^\infty(\bar{n}, \bar{x}, \lambda \bar{x}' \Phi^\infty(\bar{x}', \bar{f}), \bar{f}) \\ &= \lambda \bar{x} \Phi(\bar{x}, \lambda \bar{x}' \Phi^\infty(\bar{x}', \bar{f}), \bar{f}) \\ &= \lambda \bar{x} \Phi^\infty(\bar{x}, \bar{f}). \end{aligned}$$

For the other direction, prove by induction on ξ (using monotonicity again) that

$$\Psi^\xi(\bar{u}, \bar{x}, \lambda \bar{x}' X^\infty(\bar{n}, \bar{x}', \bar{f}), \bar{f}) = w \Rightarrow X^\infty(\bar{u}, \bar{x}, \bar{f}) = w,$$

so that

$$\begin{aligned} \lambda \bar{y} \Psi^\infty(\bar{n}, \bar{x}, \lambda \bar{x}' X^\infty(\bar{n}, \bar{x}', \bar{f}), \bar{f}) &= \lambda \bar{x} \Phi(\bar{x}, \lambda \bar{x}' X^\infty(\bar{n}, \bar{x}', \bar{f}), \bar{f}) \\ &\subseteq \lambda \bar{x}' X^\infty(\bar{n}, \bar{x}', \bar{f}); \end{aligned}$$

by the minimality of Φ^∞ then (see 2.1)

$$\lambda \bar{x} \Phi^\infty(\bar{x}, \bar{f}) \subseteq \lambda \bar{x}' X^\infty(\bar{n}, \bar{x}', \bar{f})$$

and we are done. $\square$

As a simple application of this theorem, we can now eliminate the assumption that $\varphi(a) = a \div 1$ is in $\mathcal{J}$ from the proof that the class of $\mathcal{J}$ -recursive functionals is closed under primitive recursion (see 2.4).

Indeed the Induction Completeness Theorem tells us that it is sufficient to show that $a \div 1$ is $\mathcal{J}$ -recursive. But

$$a \div 1 =_{\mathcal{J}} \begin{cases} 0 & \text{if } a = 0, \\ \mu i [i + 1 = a] & \text{if } a \in \omega, a \neq 0, \\ 0 & \text{if } a \notin \omega, \end{cases}$$

so $a \div 1$ is $\mathcal{J}$ -recursive.

4. Relations with ordinary recursion theory

Before we proceed to develop further the theory of functional induction, we will consider in this and the next section some interesting examples and we will establish connections with some classical aspects of recursion theory.

4.1. Let A be an infinite set and suppose that $\omega \subseteq B \subseteq A$. A functional $\Phi(\bar{x}, \bar{f})$ on A *concentrates* on B if for each $\bar{x} \in B^n$ and each $\bar{f} = (f_1 \cdots f_m) \in \mathcal{P}\mathcal{J}_{k_1}(A) \times \cdots \times \mathcal{P}\mathcal{J}_{k_m}(A)$ we have

$$\Phi(\bar{x}, \bar{f}) = \Phi(\bar{x}, \bar{f} \upharpoonright B),$$

where $\bar{f} \upharpoonright B = (f_1 \upharpoonright B^{k_1}, \dots, f_m \upharpoonright B^{k_m})$. If $\mathcal{J}$ is a class of functionals on A , let $\mathcal{J} \upharpoonright B$ be the class of all functionals *on* B which are restrictions to B of functionals in $\mathcal{J}$ which concentrate on B . Here the *restriction* $\Phi \upharpoonright B$ of a functional $\Phi(\bar{x}, \bar{f})$ on A is the functional on B defined by

$$\Phi \upharpoonright B(\bar{x}, \bar{f}) = \Phi(\bar{x}, \bar{f})$$

for $\bar{x} \in B^n$, $f \in \mathcal{P}\mathcal{J}_{k_1}(B) \times \cdots \times \mathcal{P}\mathcal{J}_{k_m}(B)$ and we have

$$\mathcal{J} \upharpoonright B = \{\Phi \upharpoonright B : \Phi \in \mathcal{J}, \Phi \text{ concentrates on } B\}.$$

Notice that if $\mathcal{J}$ is a suitable class of functionals on A , then $\mathcal{J} \upharpoonright B$ is a suitable class of functionals on B .

For example, every functional in $\mathcal{J}_0(A)$ = smallest suitable class of functionals on A , concentrates on B , so

$$\mathcal{J}_0(A) \upharpoonright B = \mathcal{J}_0(B).$$

More generally, if $\mathcal{J} = \mathcal{J}_0(A)[\bar{\Phi}]$, where each functional in $\bar{\Phi}$ concentrates on B , then $\mathcal{J}_0(A)[\bar{\Phi}] \upharpoonright B = \mathcal{J}_0(B)[\bar{\Phi} \upharpoonright B]$, where if $\bar{\Phi} = (\Phi_1 \cdots \Phi_n)$, then $\bar{\Phi} \upharpoonright B = (\Phi_1 \upharpoonright B \cdots \Phi_n \upharpoonright B)$. Notice also here that if every functional in $\mathcal{J}$ concentrates on B then the $\mathcal{J} \upharpoonright B$ -recursive functionals are just the restrictions to B of the $\mathcal{J}$ -recursive functionals.

Specializing the above to the case $B = \omega$ we see that for any A the $\mathcal{J}_0(A) \upharpoonright \omega$ -recursive functions are just the $\mathcal{J}_0(\omega)$ -recursive functions. It is now easy to identify these as follows:

4.2. THEOREM. *A partial function $f : \omega^n \rightarrow \omega$ is $\mathcal{J}_0$ -recursive if and only if it is recursive.*

PROOF. That every recursive partial function on ω is $\mathcal{J}_0$ -recursive is obvious from the closure properties of the class of $\mathcal{J}_0$ -recursive partial functions. For the converse, notice that if $\Phi(\bar{x}, f)$ is an operative functional in $\mathcal{J}_0$, then the associated operator $\Theta(f) = \lambda \bar{x} \Phi(\bar{x}, f)$ is a recursive operator in the sense of ordinary recursion theory, so its least fixed point $\Phi^\infty(\bar{x})$ is recursive by the Kleene First Recursion Theorem (see ROGERS [1967]). $\square$

5. Recursion in type 2 objects and quantifiers

We will give in this section a number of important types of functionals relative to which we want to study recursion.

5.1. Let A be an infinite set with $\omega \subseteq A$. A *type 2 object on A* is a total mapping

$$F : \omega^A \rightarrow \omega,$$

where ω^A is the set of all total functions from A into ω . Every type 2 object F can be naturally identified with a functional of signature $(0, 1)$ on A , namely

$$F(f) = \begin{cases} F(f) & \text{if } f : A \rightarrow \omega \text{ is total,} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Clearly this is monotone since if $f \subseteq g$ and $F(f) = w$, then f is total so also g is total and thus $f = g$, therefore $F(g) = w$.

Of particular interest is the type 2 object $E = E_A$ which embodies existential quantification over A :

$$E(f) = \begin{cases} 0 & \text{if } \exists x (f(x) = 0), \\ 1 & \text{if } \forall x (f(x) \neq 0). \end{cases}$$

Another interesting type 2 object is the *Tugué* object E_1 . This is defined

relative to a coding of tuples on A , i.e. a 1-1 mapping $\langle \rangle: \bigcup_n A^n \rightarrow A$. For each total f ,

$$E_1(f) = \begin{cases} 0 & \text{if } \exists a_0, a_1, \dots \forall n (f(\langle a_0 \cdots a_n \rangle) = 0), \\ 1 & \text{if } \forall a_0, a_1, \dots \exists n (f(\langle a_0 \cdots a_n \rangle) \neq 0). \end{cases}$$

To illustrate the present ideas and establish a further connection with classical notions in recursion theory we will consider in some detail recursion in $E = E_\omega$. We need a definition first.

5.2. DEFINITION. Let $\mathcal{J}$ be a suitable class of functionals on A . A relation $R \subseteq A^n$ is $\mathcal{J}$ -semirecursive if there is an $\mathcal{J}$ -recursive partial function $f: A^n \rightarrow \omega$ such that

$$R = \text{domain}(f).$$

i.e.

$$\begin{aligned} R(\bar{x}) &\Leftrightarrow f(\bar{x}) \downarrow \\ &\Leftrightarrow f(\bar{x}) \text{ is defined.} \end{aligned}$$

In case $\mathcal{J} = \mathcal{J}_0[\bar{\Phi}]$, we will call the $\mathcal{J}$ -semirecursive relations simply *semirecursive in $\bar{\Phi}$* . In case $A = \omega$, $\bar{\Phi} = \emptyset$, this terminology agrees with the classical one in view of 4.2. We now have:

5.3. THEOREM (KLEENE [1959]). Let E be the type 2 object which embodies existential quantification on ω . A relation on ω is semirecursive in E if and only if it is Π_1^1 .

PROOF. Let $R(\bar{x})$ be semirecursive in E and let $\Phi(\bar{u}, \bar{x}, f) \in \mathcal{J}_0[E]$ be such that for some fixed $\bar{n}$,

$$R(\bar{x}) \Leftrightarrow \Phi^\infty(\bar{n}, \bar{x}) \downarrow.$$

Then

$$\begin{aligned} R(\bar{x}) &\Leftrightarrow \exists k (\Phi^\infty(\bar{n}, \bar{x}) = k) \\ &\Leftrightarrow \exists k \forall f [\forall \bar{u}' \bar{x}' (\Phi(\bar{u}', \bar{x}', f) = f(\bar{u}', \bar{x}')) \Rightarrow f(\bar{n}, \bar{x}) = k]. \end{aligned}$$

Identifying partial functions on ω with their graphs we can easily calculate that R is Π_1^1 .

For the converse, assume $R(\bar{x})$ is a Π_1^1 relation, say

$$R(\bar{x}) \Leftrightarrow \forall \alpha \exists n P(\bar{x}, \bar{\alpha}(n)).$$

Here α varies over ω^ω , $\bar{\alpha}(n) = \langle \alpha(0) \cdots \alpha(n-1) \rangle$ with

$$\langle k_0 \cdots k_{n-1} \rangle = p_0^{k_0+1} \cdot p_1^{k_1+1} \cdots p_{n-1}^{k_{n-1}+1},$$

where $p_i = i$ -th prime and $P(\bar{x}, u)$ is a recursive relation with the property that if $P(\bar{x}, \bar{\alpha}(n))$ & $m \geq n$, then $P(\bar{x}, \bar{\alpha}(m))$. Define

$$\Psi(u, \bar{x}, f) = \begin{cases} 0 & \text{if } P(\bar{x}, u) \text{ \& Seq}(u), \\ 1 \div E(\lambda t(1 \div f(u * t, \bar{x}))) & \text{if } \neg P(\bar{x}, u) \vee \neg \text{Seq}(u), \end{cases}$$

where $\text{Seq}(u) \Leftrightarrow \exists k_0 \cdots k_{n-1} (u = \langle k_0 \cdots k_{n-1} \rangle)$ and

$$u * t = \begin{cases} \langle k_0 \cdots k_{n-1} t \rangle & \text{if } u = \langle k_0 \cdots k_{n-1} \rangle \text{ for some } k_0 \cdots k_{n-1}, \\ 0 & \text{if } \neg \text{Seq}(u). \end{cases}$$

By convention $1 = \langle \rangle =$ code of the empty sequence, so that $\text{Seq}(1)$. Since $\text{Seq}, *$ are recursive, it follows that Ψ is recursive in E , so by the Induction Completeness Theorem 3.3, $\Psi^\infty(u, \bar{x})$ is also recursive in E . It is easy now to check by induction on ξ that if $\text{Seq}(u)$ then

$$\Psi^\xi(u, \bar{x}) = 0 \Rightarrow \forall \alpha \supseteq u \exists n P(\bar{x}, \bar{\alpha}(n)),$$

where $\alpha \supseteq u \Leftrightarrow \exists t (\bar{\alpha}(t) = u)$. On the other hand if $\Psi^\infty(u, \bar{x})$ is undefined or defined and $\neq 0$, then $\neg P(\bar{x}, u)$ holds, so for some t , $\Psi^\infty(u * t, \bar{x})$ is undefined or is $\neq 0$. Repeating this we get an $\alpha \supseteq u$ such that for all n , $\neg P(\bar{x}, \bar{\alpha}(n))$, so for $\bar{\text{Seq}}(u)$ we have

$$\Psi^\infty(u, \bar{x}) = 0 \Leftrightarrow \forall \alpha \supseteq u \exists n P(\bar{x}, \bar{\alpha}(n)),$$

therefore $R(\bar{x}) \Leftrightarrow \Psi^\infty(1, \bar{x}) = 0$. Thus $R = \text{domain}(\varphi)$, where

$$\varphi(\bar{x}) = \begin{cases} 0 & \text{if } \Psi^\infty(1, \bar{x}) = 0, \\ \text{undefined} & \text{if } \Psi^\infty(1, \bar{x}) \neq 0, \end{cases}$$

and R is semirecursive in E . $\square$

We shall prove in Section 9 that a function φ is recursive in E exactly when its graph is Π_1^1 .

5.4. The second type of functionals we are going to consider here originates in the notion of a quantifier.

A *quantifier* on a set A is a collection Q of subsets of A with the monotonicity property

$$X \subseteq Y \subseteq A \text{ \& } X \in Q \Rightarrow Y \in Q.$$

To avoid trivialities we assume also that $\emptyset \subsetneq Q \subsetneq \text{power set of } A$. It is customary when dealing with quantifiers to write interchangeably

$$\{x: R(x)\} \in Q \Leftrightarrow Q(\{x: R(x)\}) \Leftrightarrow Qx R(x).$$

The *dual quantifier* to Q is defined by

$$\check{Q}x R(x) \Leftrightarrow \neg Qx \neg R(x),$$

i.e.,

$$X \in \check{Q} \Leftrightarrow (A - X) \notin Q.$$

The standard examples of quantifiers are of course the *existential quantifier* $\exists = \exists_A = \{X \subseteq A: X \neq \emptyset\}$ and its dual, the *universal quantifier* $\forall = \forall_A = \{A\}$. Another interesting quantifier is the *Suslin quantifier* (relative to a coding of tuples on A),

$$\mathcal{S}x R(x) \Leftrightarrow \forall x_0 \forall x_1 \cdots \exists k R(\langle x_0 \cdots x_k \rangle).$$

Every quantifier Q can be essentially identified with the type 2 object F_Q defined as follows: for total $f: A \rightarrow \omega$

$$F_Q(f) = \begin{cases} 0 & \text{if } Qx (f(x) = 0), \\ 1 & \text{if } \check{Q}x (f(x) \neq 0). \end{cases}$$

Under this identification E corresponds to $\exists$ and E_1 to $\check{\mathcal{S}}$. Of course there are many type 2 objects which do not correspond to quantifiers.

Every quantifier Q gives also rise to another functional of signature $(0, 1)$ F_Q^* ,

$$F_Q^*(f) = \begin{cases} 0 & \text{if } Qx (f(x) = 0), \\ 1 & \text{if } \check{Q}x (f(x) \neq 0), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

For example (recalling that $F_\exists = E$),

$$E^*(f) = \begin{cases} 0 & \text{if } \exists x (f(x) = 0), \\ 1 & \text{if } \forall x (f(x) \neq 0), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Clearly F_Q is the restriction of F_Q^* to total $f: A \rightarrow \omega$ and it is not hard to see that F_Q is recursive in F_Q^* , E^* . Indeed,

$$F_Q(f) = F_Q^*(f) \cdot \Psi(f),$$

where

$$\Psi(f) = \begin{cases} 1 & \text{if } f \text{ is total,} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Now Ψ is recursive in E^* since $\Psi(f) = E^*(\lambda x (f(x) + 1))$. In particular E is recursive in E^* so that every function recursive in E is also recursive in E^* .

In general, for most A , there are functions recursive in $E^\#$ which are not recursive in E . An exception is $A = \omega$, in which case the functions recursive in E and $E^\#$ both coincide with the functions with Π_1^1 graph; see 5.3 and 9.5.

For those familiar with the theory of inductive definability we mention the fact that if $\mathfrak{A} = \langle A, R_1 \cdots R_l \rangle$ is an acceptable structure, then a relation on A is semirecursive in $F_\alpha^\#, E^\#$ and the characteristic functions of $=, R_1 \cdots R_l$ if and only if it is absolutely $\mathcal{L}^{\mathfrak{A}}(\mathbf{Q})$ -inductive. For the definitions, see MOSCHOVAKIS [1974a].

Recursion relative to F_α and $F_\alpha^\#$ for quantifiers $\mathbf{Q}$ on ω was introduced by HINMAN [1969], who also established there its main properties (including the version of 7.2 in the context of recursion in $F_\alpha^\#$). See also ACZEL [1970].

6. The Stage Comparison Theorem

6.1. Let $\Phi(\bar{x}, f)$ be an operative functional on A . Consider $\Phi^\infty(\bar{x})$ and associate with each $\bar{x}$ for which $\Phi^\infty(\bar{x})$ is defined the ordinal

$$|\bar{x}|_\Phi = \text{least } \xi \text{ such that } \Phi^\xi(\bar{x}) \downarrow.$$

We also agree to put

$$|\bar{x}|_\Phi = \infty = \text{card}(A)^+,$$

when $\Phi^\infty(\bar{x}) \uparrow$, where

$$f(\bar{x}) \uparrow \Leftrightarrow f(\bar{x}) \text{ is not defined.}$$

Thus,

$$|\bar{x}|_\Phi < \infty \Leftrightarrow \Phi^\infty(\bar{x}) \downarrow.$$

Given now two operative functionals $\Phi(\bar{x}, f), \Psi(\bar{y}, g)$ let

$$\bar{x} \leq_{\Phi, \Psi}^* \bar{y} \Leftrightarrow \Phi^\infty(\bar{x}) \downarrow \ \& \ |\bar{x}|_\Phi \leq |\bar{y}|_\Psi,$$

$$\bar{x} <_{\Phi, \Psi}^* \bar{y} \Leftrightarrow \Phi^\infty(\bar{x}) \downarrow \ \& \ |\bar{x}|_\Phi < |\bar{y}|_\Psi \Leftrightarrow |\bar{x}|_\Phi < |\bar{y}|_\Psi,$$

and put

$$\chi(\bar{x}, \bar{y}) = \begin{cases} 0 & \text{if } \bar{x} \leq_{\Phi, \Psi}^* \bar{y}, \\ 1 & \text{if } \bar{y} <_{\Phi, \Psi}^* \bar{x}; \end{cases}$$

we call χ the *stage comparison* partial function for Φ, Ψ .

If Φ, Ψ are in some suitable class $\mathcal{J}$, it is natural to ask whether the associated χ is $\mathcal{J}$ -recursive. This fails in general, but holds when Φ and Ψ are normal according to the following definition due to MOSCHOVAKIS [1976].

6.2. DEFINITION. Let $\mathcal{F}$ be a class of functionals on A and let $\Phi(\bar{x}, \bar{f})$ be a functional in $\mathcal{F}$. We call Φ *normal* in $\mathcal{F}$ if there is an $\mathcal{F}$ -recursive functional $\Delta_\Phi(\bar{x}, \bar{f}, \bar{\delta})$ taking values 0, 1 only such that

(i) if $\Phi(\bar{x}, \bar{f} \upharpoonright \{\bar{y}: \bar{\delta}(\bar{y}) = 0\}) \downarrow$, then $\Delta_\Phi(\bar{x}, \bar{f}, \bar{\delta}) = 0$,

(ii) if $\bar{\delta}$ is total, $\{\bar{y}: \bar{\delta}(\bar{y}) = 0\} \subseteq \text{domain}(\bar{f})$, and $\Phi(\bar{x}, \bar{f} \upharpoonright \{\bar{y}: \bar{\delta}(\bar{y}) = 0\}) \uparrow$, then $\Delta_\Phi(\bar{x}, \bar{f}, \bar{\delta}) = 1$.

Here the vector notation is used in the obvious way: if $\bar{f} = (f_1 \cdots f_m) \in \mathcal{P}\mathcal{F}_{k_1} \times \cdots \times \mathcal{P}\mathcal{F}_{k_m}$, then $\bar{\delta} = (\delta_1 \cdots \delta_m)$ varies also over $\mathcal{P}\mathcal{F}_{k_1} \times \cdots \times \mathcal{P}\mathcal{F}_{k_m}$,

$$\bar{f} \upharpoonright \{\bar{y}: \bar{\delta}(\bar{y}) = 0\} = (f_1 \upharpoonright \{\bar{y}_1: \delta_1(\bar{y}_1) = 0\}, \dots, f_m \upharpoonright \{\bar{y}_m: \delta_m(\bar{y}_m) = 0\})$$

and $\{\bar{y}: \bar{\delta}(\bar{y}) = 0\} \subseteq \text{domain}(\bar{f})$ means that for all $1 \leq i \leq m$, $\{\bar{y}_i: \delta_i(\bar{y}_i) = 0\} \subseteq \text{domain}(f_i)$.

We call a class of functionals $\mathcal{F}$ *normal* if every functional in $\mathcal{F}$ is normal in $\mathcal{F}$.

The following result is due to MOSCHOVAKIS [1976] and its proof is patterned after a proof of Aczel–Kunen of a similar result in positive elementary inductive definability; see MOSCHOVAKIS [1974a].

6.3. THE STAGE COMPARISON THEOREM. *Let $\mathcal{F}$ be a suitable class of functionals on A and let $\Phi(\bar{x}, f)$, $\Psi(\bar{y}, g)$ be two functionals in $\mathcal{F}$ which are normal in $\mathcal{F}$; then the stage comparison function of Φ , Ψ is $\mathcal{F}$ -recursive.*

PROOF. Let $\Delta_\Phi(\bar{x}, f, \delta)$, $\Delta_\Psi(\bar{y}, g, \varepsilon)$ be the functionals associated with Φ , Ψ in the definition of normality 6.2. We will find a functional $X(\bar{x}, \bar{y}, h)$ with values 0, 1 whose least fixed point $X^\infty(\bar{x}, \bar{y})$ has the property that if $\bar{x} \leq_{\Phi, \Psi}^* \bar{y}$, then $X^\infty(\bar{x}, \bar{y}) = 0$ and if $\bar{y} <_{\Psi, \Phi}^* \bar{x}$, then $X^\infty(\bar{x}, \bar{y}) = 1$. From this we can easily get the stage comparison function,

$$\chi(\bar{x}, \bar{y}) = \begin{cases} \Phi^\infty(\bar{x}) \cdot 0 & \text{if } X^\infty(\bar{x}, \bar{y}) = 0, \\ \varphi(\Psi^\infty(\bar{y})) & \text{if } X^\infty(\bar{x}, \bar{y}) = 1, \end{cases}$$

where $\varphi(a) = 1$ for all a .

Heuristically, X is found as follows: dropping subscripts to simplify the notation,

$$\begin{aligned} \bar{x} \leq_{\Phi, \Psi}^* \bar{y} &\Leftrightarrow \Phi^{|\bar{y}|}(\bar{x}) \downarrow \Leftrightarrow \Phi(\bar{x}, \Phi^{<|\bar{y}|}) \downarrow \\ &\Leftrightarrow \Phi(\bar{x}, \Phi^\infty \upharpoonright \{\bar{x}': |\bar{x}'| < |\bar{y}|\}) \downarrow. \end{aligned}$$

Now

$$|\bar{x}'| < |\bar{y}| \Rightarrow \Psi^{|\bar{x}'|}(\bar{y}) \uparrow \Leftrightarrow \Psi(\bar{y}, \Psi^{<|\bar{x}'|}) \uparrow.$$

Thus letting

$$\dot{\neg} h(\bar{z}) = \begin{cases} 1 & \text{if } h(\bar{z}) = 0, \\ 0 & \text{if } h(\bar{z}) = 1, \end{cases}$$

we have

$$\begin{aligned} \chi(\bar{x}, \bar{y}) = 0 &\Rightarrow \Phi(\bar{x}, \Phi^\infty \upharpoonright \{\bar{x}': \Psi(\bar{y}, \Psi^\infty \upharpoonright \{\bar{y}': |\bar{y}'| < |\bar{x}'|\}) \uparrow\}) \downarrow \\ &\Rightarrow \Delta_\Phi(\bar{x}, \Phi^\infty, \lambda \bar{x}' \dot{\neg} \Delta_\Psi(\bar{y}, \Psi^\infty, \lambda \bar{y}' \dot{\neg} \chi(\bar{x}', \bar{y}')))) = 0. \end{aligned}$$

Similary

$$\chi(\bar{x}, \bar{y}) = 1 \Rightarrow \Delta_\Phi(\bar{x}, \Phi^\infty, \lambda \bar{x}' \dot{\neg} \Delta_\Psi(\bar{y}, \Psi^\infty, \lambda \bar{y}' \dot{\neg} \chi(\bar{x}', \bar{y}')))) = 1.$$

So if $\Phi^\infty(\bar{x}) \downarrow$ or $\Psi^\infty(\bar{y}) \downarrow$ we have

$$\chi(\bar{x}, \bar{y}) = \Delta_\Phi(\bar{x}, \Phi^\infty, \lambda \bar{x}' \dot{\neg} \Delta_\Psi(\bar{y}, \Psi^\infty, \lambda \bar{y}' \dot{\neg} \chi(\bar{x}', \bar{y}')))).$$

This suggests taking

$$X(\bar{x}, \bar{y}, h) = \Delta_\Phi(\bar{x}, \Phi^\infty, \lambda \bar{x}' \dot{\neg} \Delta_\Psi(\bar{y}, \Psi^\infty, \lambda \bar{y}' \dot{\neg} h(\bar{x}', \bar{y}')))).$$

Clearly X is an $\mathcal{J}$ -recursive functional by the Substitution Theorem 3.2, so by the Completeness Theorem 3.3, $X^\infty(\bar{x}, \bar{y})$ is also $\mathcal{J}$ -recursive. To prove that X^∞ has the required properties one proves first by induction on ξ that

$$\bar{x} \leq_{\Phi, \Psi}^* \bar{y} \ \& \ |\bar{x}|_\Phi = \xi \Rightarrow X^\xi(\bar{x}, \bar{y}) = 0$$

and then again by induction on ξ that

$$\bar{y} <_{\Psi, \Phi}^* \bar{x} \ \& \ |\bar{y}|_\Psi = \xi \Rightarrow X^\xi(\bar{x}, \bar{y}) = 1.$$

We leave the details to the reader. $\square$

We will see in a moment that the examples of functionals we discussed in Section 5 lead to normal classes, but let us first establish the following simple criterion for normality.

6.4. PROPOSITION. *Let $\bar{\Phi}$ be a finite sequence of functionals on A ; if every functional in the list $\bar{\Phi}$ is normal in $\mathcal{J}_0[\bar{\Phi}]$, then $\mathcal{J}_0[\bar{\Phi}]$ is normal.*

PROOF. Assume that every functional in $\bar{\Phi}$ is normal in $\mathcal{J}_0[\bar{\Phi}]$. We prove that every functional in $\mathcal{J}_0[\bar{\Phi}]$ is normal in $\mathcal{J}_0[\bar{\Phi}]$ by induction on the construction of $\mathcal{J}_0[\bar{\Phi}]$.

Cases 2.3(i)–(v), i.e., the initial functionals, are trivial. For example if $\Phi(\bar{x}, f) = f(\bar{x})$ we take

$$\Delta_{\Phi}(\bar{x}, f, \delta) = \begin{cases} 0 & \text{if } \delta(\bar{x}) = 0, \\ 1 & \text{if } \delta(\bar{x}) \neq 0. \end{cases}$$

Also 2.3(vi), (viii), (ix), (x) are straightforward. Finally, for 2.3(vii), assuming that for $\Phi(a, \bar{x}, \bar{f})$, $X(\bar{x}, \bar{f})$ we have already found Δ_{Φ} , Δ_X with the required properties and letting $\Psi(\bar{x}, \bar{f}) = \Phi(X(\bar{x}, \bar{f}), \bar{x}, \bar{f})$, we take

$$\Delta_{\Psi}(\bar{x}, \bar{f}, \bar{\delta}) = \begin{cases} \Delta_{\Phi}(X(\bar{x}, \bar{f}), \bar{x}, \bar{f}, \bar{\delta}) & \text{if } \Delta_X(\bar{x}, \bar{f}, \bar{\delta}) = 0, \\ \Delta_X(\bar{x}, \bar{f}, \bar{\delta}) & \text{if } \Delta_X(\bar{x}, \bar{f}, \bar{\delta}) \neq 0. \quad \square \end{cases}$$

Call a finite sequence of functionals $\bar{\Phi}$ on A *normal* if each functional in $\bar{\Phi}$ is normal in $\mathcal{I}_0[\bar{\Phi}]$.

6.5. THEOREM. (i) *For every finite sequence $\bar{F}$ of type 2 objects on A the extended sequence $\bar{F}$, E is normal.*

(ii) *Let Q be a quantifier on A ; then $F_Q^{\#}$ is normal.*

PROOF. (i) To each type 2 object F in $\bar{F}$ assign the same

$$\Delta_F(f, \delta) = 1 \div E(\lambda x (1 \div \delta(x))),$$

where

$$1 \div a = \begin{cases} 1 & \text{if } a = 0, \\ 0 & \text{if } a \neq 0 \text{ or } a \notin \omega. \end{cases}$$

(ii) Let Q be a quantifier on A and let $\Phi = F_Q^{\#}$ be the associated functional. Put first

$$\Psi(x, f, \delta) = \begin{cases} 1 & \text{if } \delta(x) \neq 0, \\ 1 & \text{if } \delta(x) = 0, f(x) \neq 0, \\ 0 & \text{if } \delta(x) = 0, f(x) = 0, \end{cases}$$

and

$$X(x, f, \delta) = \begin{cases} 0 & \text{if } \delta(x) \neq 0, \\ 1 & \text{if } \delta(x) = 0, f(x) \neq 0, \\ 0 & \text{if } \delta(x) = 0, f(x) = 0. \end{cases}$$

Now let

$$\Delta_{\Phi}(f, \delta) = \begin{cases} 0 & \text{if } F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 0, \\ 0 & \text{if } F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 1 \text{ \& } F_Q^{\#}(\lambda x X(x, f, \delta)) = 1, \\ 1 & \text{if } F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 1 \text{ \& } F_Q^{\#}(\lambda x X(x, f, \delta)) = 0. \end{cases}$$

To prove that Δ_{Φ} works assume first that $F_Q^{\#}(f \upharpoonright \{x: \delta(x) = 0\}) \downarrow$. Then either $Qx (f(x) = 0 \text{ \& } \delta(x) = 0)$ or $\bar{Q}x (f(x) \neq 0 \text{ \& } \delta(x) = 0)$. In the first

case $F_{\alpha}^{\#}(\lambda x \Psi(x, f, \delta)) = 0$ and in the second $F_{\alpha}^{\#}(\lambda x \Psi(x, f, \delta)) = 1$ and $F_{\alpha}^{\#}(\lambda x X(x, f, \delta)) = 1$, so that in either case $\Delta_{\phi}(f, \delta) = 0$. If now δ is total, $\{x: \delta(x) = 0\} \subseteq \text{domain}(f)$ and $F_{\alpha}^{\#}(f \upharpoonright \{x: \delta(x) = 0\}) \uparrow$ then we must have that both $Qx (f(x) = 0 \ \& \ \delta(x) = 0)$ and $\check{Q}x (f(x) \neq 0 \ \& \ \delta(x) = 0)$ fail, so that $\check{Q}x (f(x) \neq 0 \vee f(x) \uparrow \vee \delta(x) \neq 0)$ and $Qx (f(x) = 0 \vee f(x) \uparrow \vee \delta(x) \neq 0)$ hold. Noticing that $f(x) \uparrow \Rightarrow \delta(x) \neq 0$ we have $\check{Q}x (f(x) \neq 0 \vee \delta(x) \neq 0)$ and $Qx (f(x) = 0 \vee \delta(x) \neq 0)$, so that $F_{\alpha}^{\#}(\lambda x \Psi(x, f, \delta)) = 1$ and $F_{\alpha}^{\#}(\lambda x X(x, f, \delta)) = 0$ i.e. $\Delta_{\phi}(f, \delta) = 1$. $\square$

7. Semirecursive relations

7.1. Let $\mathcal{F}$ be a class of functionals on A and recall from 5.2 that a relation $R \subseteq A^n$ is called $\mathcal{F}$ -semirecursive if it is the domain of an $\mathcal{F}$ -recursive partial function $\varphi: A^n \rightarrow \omega$. We call a relation $R \subseteq A^n$ $\mathcal{F}$ -recursive if its characteristic function

$$\chi_R(\bar{x}) = \begin{cases} 0 & \text{if } R(\bar{x}), \\ 1 & \text{if } \neg R(\bar{x}), \end{cases}$$

is $\mathcal{F}$ -recursive, where $\neg R = A^n - R$.

Here we discuss some structure and closure properties of the class of $\mathcal{F}$ -semirecursive relations for suitable, normal $\mathcal{F}$. This study will be completed in Section 9 after we prove enumeration.

Given a relation $R \subseteq A^n$, a *norm* on R is a map $\sigma: R \rightarrow \text{ordinals}$. We also agree to put $\sigma(\bar{x}) = \infty$ = an ordinal bigger than all $\sigma(\bar{y})$ with $R(\bar{y})$, if $\neg R(\bar{x})$ holds. To each norm σ on R we associate the relations

$$\bar{x} \leq_{\sigma}^* \bar{y} \Leftrightarrow R(\bar{x}) \ \& \ \sigma(\bar{x}) \leq \sigma(\bar{y})$$

$$\bar{x} <_{\sigma}^* \bar{y} \Leftrightarrow R(\bar{x}) \ \& \ \sigma(\bar{x}) < \sigma(\bar{y}) \Leftrightarrow \sigma(\bar{x}) < \sigma(\bar{y})$$

If Γ is a collection of relations on A and σ is a norm on R we call σ a Γ -norm if both $\leq_{\sigma}^*$, $<_{\sigma}^*$ are in Γ . We say that Γ itself is *normed* or has the *prewellordering property* if every relation in Γ admits a Γ -norm.

7.2. THE PREWELLORDERING THEOREM. *Let $\mathcal{F}$ be a suitable, normal class of functionals on A . Then the class of $\mathcal{F}$ -semirecursive relations is normed.*

PROOF. Let $R(\bar{x}) \Leftrightarrow \varphi(\bar{x}) \downarrow$, where φ is $\mathcal{F}$ -recursive, let $\varphi(\bar{x}) = \Phi^{\infty}(\bar{n}, \bar{x})$, with $\Phi \in \mathcal{F}$ and put $\sigma(\bar{x}) = |\bar{n}, \bar{x}|_{\Phi}$ (see 6.1). Then σ is an $\mathcal{F}$ -semirecursive norm on R by the Stage Comparison Theorem 6.3. $\square$

A class of relations Γ on A is *closed under* $\vee$ if for all $R, S \subseteq A^n$ in Γ , the relation

$$(R \vee S)(\bar{x}) \Leftrightarrow R(\bar{x}) \vee S(\bar{x})$$

is also in Γ . Similarly for $\&$ and $\neg$

7.3. THEOREM. *Let $\mathcal{J}$ be a suitable, normal class of functionals on A . Then*

- (i) *The class of $\mathcal{J}$ -semirecursive relations is closed under $\&$, $\vee$.*
- (ii) *A relation R is $\mathcal{J}$ -recursive if and only if both R and $\neg R$ are $\mathcal{J}$ -semirecursive.*

PROOF. (i) Closure under $\&$ is easy and does not need normality. This is because

$$\varphi(\bar{x}) \downarrow \& \psi(\bar{x}) \downarrow \Leftrightarrow (\varphi(\bar{x}) + \psi(\bar{x})) \downarrow.$$

For $\vee$, let

$$R(\bar{x}) \Leftrightarrow \varphi(\bar{x}) \downarrow, \quad S(\bar{x}) \Leftrightarrow \psi(\bar{x}) \downarrow$$

with φ, ψ $\mathcal{J}$ -recursive. By the Stage Comparison Theorem we can get a function $\chi(\bar{x}_1, \bar{x}_2)$, where $\bar{x}_1, \bar{x}_2 \in A^n$, which is defined exactly when either $\varphi(\bar{x}_1) \downarrow$ or $\varphi(\bar{x}_2) \downarrow$. Then

$$R(\bar{x}) \vee S(\bar{x}) \Leftrightarrow \chi(\bar{x}, \bar{x}) \downarrow$$

and we are done.

(ii) Assume $R, \neg R$ are $\mathcal{J}$ -semirecursive. Let $R(\bar{x}) \Leftrightarrow \varphi(\bar{x}) \downarrow$, $\neg R(\bar{x}) \Leftrightarrow \psi(\bar{x}) \downarrow$ and find again $\chi(\bar{x}_1, \bar{x}_2)$ $\mathcal{J}$ -recursive such that if $\varphi(\bar{x}_1) \downarrow$ and $\psi(\bar{x}_2) \uparrow$, then $\chi(\bar{x}_1, \bar{x}_2) = 0$ and if $\psi(\bar{x}_2) \downarrow$ and $\varphi(\bar{x}_1) \uparrow$ then $\chi(\bar{x}_1, \bar{x}_2) = 1$. Then we must have $\chi_R(\bar{x}) = \chi(\bar{x}, \bar{x})$, so R is $\mathcal{J}$ -recursive. $\square$

For example in view of 6.5 and 5.3 we have that a relation on ω is recursive in E if and only if it is Δ_1^1 , i.e. hyperarithmetical (KLEENE [1959]).

8. The Enumeration Theorem

Our purpose in this section is to prove the existence of universal $\mathcal{J}$ -recursive partial functions for appropriate $\mathcal{J}$. We recall the definition first.

8.1. Let $\mathbb{F}$ be a class of partial functions (of several arguments) on A , such that $\omega \subseteq A$. We say that $\mathbb{F}$ has the *enumeration property* or is ω -

parametrized if for each $n \geq 1$ there is some $\varphi(a, x_1 \cdots x_n)$ in $\mathbb{F}$ such that the class of all n -ary partial functions in $\mathbb{F}$ coincides with $\{\varphi_e : e \in \omega\}$, where for any partial function f ,

$$f_e(x_1 \cdots x_n) = f(e, x_1 \cdots x_n).$$

If $f = \varphi_e$, we call e a *code* or *index* of f (relative to φ). A partial function φ as above is called *universal* (for the n -ary partial functions in $\mathbb{F}$).

We will prove in 8.4 that the class of $\mathcal{J}$ -recursive partial functions has the enumeration property provided that $\mathcal{J}$ is suitable, finitely generated, and admits a coding of tuples. We now explain these notions.

8.2. Given a set A such that $\omega \subseteq A$, a *coding for tuples* on A is a one-to-one function $\mathcal{C} = \langle \rangle$ from the set of all finite sequences from A (including the empty sequence) into A . With each such coding we associate the following total functions (from A into ω) and (total) mappings from A^2 or A into A .

$$(i) \quad \chi_{\text{Seq}}(x) = \chi_{\text{Seq}}^{\mathcal{C}}(x) = \begin{cases} 0 & \text{if } \exists x_0 \cdots \exists x_{n-1} (x = \langle x_0 \cdots x_{n-1} \rangle), \\ 1 & \text{otherwise.} \end{cases}$$

$$(ii) \quad \text{lh}(x) = \text{lh}^{\mathcal{C}}(x) = \begin{cases} n & \text{if } \exists x_0 \cdots \exists x_{n-1} (x = \langle x_0 \cdots x_{n-1} \rangle), \\ 0 & \text{otherwise.} \end{cases}$$

$$(iii) \quad (x)_i = (x)_i^{\mathcal{C}} = q^{\mathcal{C}}(x, i) = \begin{cases} x_i & \text{if } \exists x_0 \cdots \exists x_{n-1} (x = \langle x_0 \cdots x_{n-1} \rangle), \\ 0 & \text{otherwise.} \end{cases}$$

$$(iv) \quad x * y = x *^{\mathcal{C}} y = \begin{cases} \langle x_0 \cdots x_{n-1} y_0 \cdots y_{m-1} \rangle & \text{if } \exists x_0 \cdots \exists x_{n-1} (x = \langle x_0 \cdots x_{n-1} \rangle) \\ & \& \exists y_0 \cdots \exists y_{m-1} (y = \langle y_0 \cdots y_{m-1} \rangle), \\ 0 & \text{otherwise.} \end{cases}$$

$$(v) \quad s(x) = s^{\mathcal{C}}(x) = \langle x \rangle.$$

Given now a class of functionals $\mathcal{J}$ on A we say that $\mathcal{J}$ *admits* the coding of tuples $\mathcal{C}$ if $\chi_{\text{Seq}}^{\mathcal{C}}, \text{lh}^{\mathcal{C}}$ are $\mathcal{J}$ -recursive and the class of $\mathcal{J}$ -recursive functionals is closed under substitution by $(x)_i^{\mathcal{C}}, x *^{\mathcal{C}} y, s^{\mathcal{C}}$. This means that if $\Phi(x, \bar{y}, \bar{f})$ is $\mathcal{J}$ -recursive and t is any of these mappings then $\Psi(\bar{z}, \bar{y}, \bar{f}) = \Phi(t(\bar{z}), \bar{y}, \bar{f})$ is also $\mathcal{J}$ -recursive.

Note now that if a suitable $\mathcal{J}$ admits the coding $\mathcal{C}$, then we can assume without loss of generality that $\mathcal{C} = \langle \rangle$ agrees with the standard coding

$$\langle k_0 \cdots k_{n-1} \rangle = p_0^{k_0+1} \cdots p_{n-1}^{k_{n-1}+1}$$

on ω . This is because if we define $\mathcal{C}' = \langle \quad \rangle'$ by

$$\langle x_0 \cdots x_{n-1} \rangle' = \begin{cases} r(\langle x_0 \cdots x_{n-1} \rangle) & \text{if at least one of } x_0 \cdots x_{n-1} \text{ is not} \\ & \text{in } \omega \text{ and } \langle x_0 \cdots x_{n-1} \rangle \in \omega, \\ \langle x_0 \cdots x_{n-1} \rangle & \text{if at least one of } x_0 \cdots x_{n-1} \text{ is not in } \omega \\ & \text{and } \langle x_0 \cdots x_{n-1} \rangle \notin \omega, \\ p_0^{x_0+1} \cdots p_{n-1}^{x_{n-1}+1} & \text{if all } x_i \text{ are in } \omega, \end{cases}$$

where $r: \omega \rightarrow \omega$ is a recursive 1-1 function whose range is recursive and avoids $\{p_0^{k_0+1} \cdots p_{n-1}^{k_{n-1}+1}; n, k_0 \cdots k_{n-1} \in \omega\}$, then $\mathcal{J}$ admits also $\mathcal{C}'$. The only nontrivial thing to check here is that the relation

$$P(x) \Leftrightarrow \chi_{\text{seq}}^{\mathcal{C}}(x) = 0 \ \& \ \forall i < \text{lh}^{\mathcal{C}}(x) ((x)_i)^{\mathcal{C}} \in \omega$$

is $\mathcal{J}$ -recursive. For that, notice that

$$\neg P(x) \Leftrightarrow \chi_{\text{seq}}^{\mathcal{C}}(x) = 1 \vee \mu i [\chi_{\omega}((x)_i)^{\mathcal{C}} = 1] < \text{lh}^{\mathcal{C}}(x).$$

From now on we will agree that any coding agrees with the standard one on ω , so that notations such as $\langle e_0 \cdots e_{n-1} \rangle$, $(e)_i$ etc. are unambiguous, if $e_i, e \in \omega$. We also agree that

$$\langle \emptyset \rangle = \text{code of empty sequence} = 1.$$

Note now that if $\mathcal{J}$ admits the coding $\mathcal{C}$, then for each fixed $n \geq 1$ the class of $\mathcal{J}$ -recursive functionals is closed under the mapping $p_n(x_0 \cdots x_{n-1}) = \langle x_0 \cdots x_{n-1} \rangle$. Also the class of $\mathcal{J}$ -recursive functionals is closed under substitutions by the mapping

$$t(x, i, j) = \begin{cases} \langle (x)_i \cdots (x)_j \rangle & \text{if } 0 \leq i \leq j \in \omega, \\ 0 & \text{otherwise.} \end{cases}$$

For that, one proves first by primitive recursion on j that if $\Phi(x, \bar{y}, \bar{f})$ is $\mathcal{J}$ -recursive then so is

$$\Psi(x, i, j, z, \bar{y}, \bar{f}) = \Phi(t(x, i, j) * z, \bar{y}, \bar{f}).$$

and then puts $z = 1 = \langle \emptyset \rangle$.

We conclude the preliminaries to the proof of the Enumeration Theorem with the following definition.

8.3. Let $\mathcal{J}$ be a suitable class of functionals. We say that $\mathcal{J}$ is *finitely generated* if there is a finite sequence of functionals $\bar{\Phi}$ and a finite sequence

of total mappings $t = (t_1 \cdots t_k)$ where $t_i : A^k \rightarrow A$, such that $\mathcal{F}$ is the smallest suitable class of functionals containing $\bar{\Phi}$ and closed under substitutions by mappings in $\bar{t}$.

8.4. THE ENUMERATION THEOREM. *Let $\mathcal{F}$ be a suitable class of functionals on A . If $\mathcal{F}$ is finitely generated and admits a coding of tuples, then the class of $\mathcal{F}$ -recursive partial functions has the enumeration property.*

PROOF. It will be clearly enough to find an $\mathcal{F}$ -recursive universal partial function $\varphi(e, x)$ for the unary $\mathcal{F}$ -recursive functions. Our plan is the following: We associate in some canonical way a code (Gödel number) $\ulcorner \Phi \urcorner \in \omega$ to each functional Φ in $\mathcal{F}$; then we construct an $\mathcal{F}$ -recursive functional $U(e, x, f)$ with f unary such that if $\ulcorner \Phi(x_1 \cdots x_n, f_1 \cdots f_m) \urcorner = e$ then

$$\Phi(x_1 \cdots x_n, f_1 \cdots f_m) = U(e, \langle x_1 \cdots x_n \rangle, \langle f_1 \cdots f_m \rangle),$$

where $\langle f_1 \cdots f_m \rangle = \lambda x \langle \tilde{f}_1(x) \cdots \tilde{f}_m(x) \rangle$, with $\tilde{f}(x) = f((x)_0 \cdots (x)_{k-1})$, if $f : A^k \rightarrow \omega$. We arrange things so that for some recursive $p : \omega \rightarrow \omega$ $p(\ulcorner \Phi(x_1 \cdots x_n, \tilde{f}) \urcorner) = n$. Then letting (for $g : A^2 \rightarrow \omega$)

$$V(e, x, g) = U(e, x, \lambda x \langle g(e, \langle (x)_0 \cdots (x)_{p(e)-1} \rangle) \rangle),$$

we have for any operative $\Phi(x_1 \cdots x_n, f)$ with $\ulcorner \Phi \urcorner = e$ and $p(e) = n$

$$\begin{aligned} \Phi(x_1 \cdots x_n, \lambda x'_1 \cdots x'_n g(e, \langle x'_1 \cdots x'_n \rangle)) &= \\ &= U(e, \langle x_1 \cdots x_n \rangle, \langle \lambda x'_1 \cdots x'_n g(e, \langle x'_1 \cdots x'_n \rangle) \rangle) \\ &= U(e, \langle x_1 \cdots x_n \rangle, \lambda x \langle g(e, \langle (x)_0 \cdots (x)_{n-1} \rangle) \rangle) \\ &= V(e, \langle x_1 \cdots x_n \rangle, g), \end{aligned}$$

so that we can prove by induction on ξ that

$$V^\xi(e, \langle x_1 \cdots x_n \rangle) = \Phi^\xi(x_1 \cdots x_n),$$

therefore

$$V^\omega(e, \langle x_1 \cdots x_n \rangle) = \Phi^\omega(x_1 \cdots x_n).$$

Then

$$\varphi(e, x) = V^\omega((e)_0, \langle (e)_1 \cdots (e)_{\text{lh}(e)-1} \rangle, x)$$

is the required universal function.

The way to define $\ulcorner \Phi \urcorner$ is more or less obvious by induction on the construction of $\mathcal{F}$. Then we define $\tilde{U}(e, x, g, f)$, by considering cases on $e = \ulcorner \Phi \urcorner$, so that $\tilde{U}^\omega(e, x, f) = U(e, x, f)$ has the required properties. It will help to notice here that since $\mathcal{F}$ is finitely generated there are finitely many

functionals $\Phi_1 \cdots \Phi_n$ in $\mathcal{J}$ and total mappings $t_1 \cdots t_k$ such that $\mathcal{J}$ is the smallest class of functionals containing $\Phi_1 \cdots \Phi_n$ which is closed under substitutions by $t_1 \cdots t_k$ and satisfies (i)–(ix) of 2.3 and (x) for $\Phi_1 \cdots \Phi_n$ only. The actual details are straightforward but a bit messy and we omit them here. $\square$

9. Consequences of enumeration

There are several corollaries of the enumeration theorem which we consider first. At the end of this section we will also look at some consequences of the enumeration theorem for the structure theory of semirecursive relations.

9.1. Let $\mathbb{F}$ be a class of partial functions on A . A *universal system* for $\mathbb{F}$ is a sequence $\{\varphi^n\}_{n \geq 1}$ of partial functions on $\mathbb{F}$ such that for each n , φ^n is $n+1$ -ary and universal for the n -ary partial functions in $\mathbb{F}$. We call $\{\varphi^n\}$ *good* if for each $n, m \geq 1$ there is a total recursive function $S_n^m(e, k_1 \cdots k_m)$ on ω such that for each $k_1 \cdots k_m \in \omega$, $x_1 \cdots x_n \in A$

$$\varphi^{m+n}(e, k_1 \cdots k_m, x_1 \cdots x_n) = \varphi^n(S_n^m(e, k_1 \cdots k_m), x_1 \cdots x_n).$$

We call these the *s-m-n functions* of $\{\varphi^n\}$. We now have:

9.2. THE s-m-n THEOREM. *Let $\mathcal{J}$ be a suitable class of functionals on A which is finitely generated and admits a coding of tuples. Then the class of $\mathcal{J}$ -recursive partial functions admits a good universal system.*

PROOF. By 8.4, let $\varphi(e, x, y)$ be an $\mathcal{J}$ -recursive partial function which is universal for the binary $\mathcal{J}$ -recursive partial functions. Then let

$$\varphi^k(e, x_1 \cdots x_k) = \varphi((e)_0, (e)_1, \langle x_1 \cdots x_k \rangle),$$

where $\mathcal{J}$ admits the coding of tuples $\langle \rangle$. Let

$$f(x, y) = \varphi^{m+n}((x)_0 \cdots (x)_m, (y)_0 \cdots (y)_{n-1})$$

and find e_0 such that

$$f(x, y) = \varphi(e_0, x, y).$$

Then

$$S_n^m(e, k_1 \cdots k_m) = \langle e_0, \langle e, k_1 \cdots k_m \rangle \rangle$$

is the required *s-m-n* function. $\square$

A basic corollary of the s - m - n theorem is:

9.3. THE (SECOND) RECURSION THEOREM. *Let $\mathcal{F}$ be a suitable, finitely generated class of functionals on A , which admits a coding of tuples. If $\{\varphi^n\}$ is a good universal system for the class of $\mathcal{F}$ -recursive partial functions, then for each $\mathcal{F}$ -recursive partial function $\psi(a, \bar{x})$ there is some $e \in \omega$ such that*

$$\varphi_e(\bar{x}) = \psi(e, \bar{x}).$$

PROOF. Let e_0 be such that $\varphi_{e_0}(a, \bar{x}) = \psi(S_n^1(a, a), \bar{x})$ and take $e = S_n^1(e_0, e_0)$. $\square$

Now we can complete the study of the general structure properties of the $\mathcal{F}$ -semirecursive relations which we started in Section 7. We say that a class of relations $\mathbb{R}$ on A is *closed under $\exists^\omega$* if for each $P(\bar{x}, a)$ in $\mathbb{R}$, the relation

$$\exists^\omega P(\bar{x}) \Leftrightarrow \exists n P(\bar{x}, n) \Leftrightarrow \exists n (n \in \omega \wedge P(\bar{x}, n))$$

is also in $\mathbb{R}$.

9.4. THEOREM. *Let $\mathcal{F}$ be a suitable, finitely generated class of functionals on A which is normal and admits a coding of tuples. Then*

- (i) *The class of $\mathcal{F}$ -semirecursive relations is closed under $\exists^\omega$.*
- (ii) *A partial function $\varphi : A^n \rightarrow \omega$ is $\mathcal{F}$ -recursive if and only if its graph is $\mathcal{F}$ -semirecursive.* $\square$

Both of these results are immediate consequences of the following basic lemma.

9.5. NUMBER SELECTION LEMMA. *If $\mathcal{F}$ is a suitable, finitely generated class of functionals on A which is normal and admits a coding of tuples, then for each $\mathcal{F}$ -semirecursive relation $P(\bar{x}, a)$ there is some $\mathcal{F}$ -recursive ψ such that*

$$\exists n P(\bar{x}, n) \Rightarrow \psi(\bar{x}) \downarrow \ \& \ P(\bar{x}, \psi(\bar{x})).$$

PROOF. Let $\varphi(e, \bar{x}, a)$ be a universal $\mathcal{F}$ -recursive partial function by 8.4. Let σ be a $\mathcal{F}$ -semirecursive norm on $W = \{(e, \bar{x}, a) : \varphi(e, \bar{x}, a) \downarrow\}$ and let $\chi(e, \bar{x}, a, e', \bar{x}', a')$ be $\mathcal{F}$ -recursive such that

$$(e, \bar{x}, a) \leq_\sigma^* (e', \bar{x}', a') \Leftrightarrow \chi(e, \bar{x}, a, e', \bar{x}', a') = 0,$$

$$(e', \bar{x}', a') <_\sigma^* (e, \bar{x}, a) \Leftrightarrow \chi(e, \bar{x}, a, e', \bar{x}', a') = 1$$

by 6.3. Then using the Recursion Theorem 9.3 we can find an $e \in \omega$ such that if

$$P(\bar{x}, a) \Leftrightarrow \varphi(e_0, \bar{x}, a) \downarrow,$$

then

$$\varphi_e(\bar{x}, a) = \begin{cases} 0 & \text{if } a \in \omega \text{ \& } \chi(e_0, \bar{x}, a, e, \bar{x}, a+1) = 0, \\ \varphi(e, \bar{x}, a+1) + 1 & \text{if } a \in \omega \text{ \& } \chi(e_0, \bar{x}, a, e, \bar{x}, a+1) = 1, \\ 0 & \text{if } a \notin \omega. \end{cases}$$

Finally, put

$$\psi(\bar{x}) = \varphi_e(\bar{x}, 0).$$

To prove that ψ works notice first that if $\varphi(e_0, \bar{x}, a) \downarrow$, then $\varphi_e(\bar{x}, a) \downarrow$ or $\varphi_e(\bar{x}, a+1) \downarrow$. Moreover if $\varphi_e(\bar{x}, b) \downarrow$, then $\varphi_e(\bar{x}, c) \downarrow$ for all $c \leq b$. Thus if $\exists a \varphi(e_0, \bar{x}, a) \downarrow$, clearly $\varphi_e(\bar{x}, 0) \downarrow$. Let a be least such that $\varphi_e(\bar{x}, a)$ is defined by the first clause above; this exists since otherwise $\varphi_e(\bar{x}, 0) = \varphi_e(\bar{x}, 1) + 1 = \varphi_e(\bar{x}, 2) + 2 = \dots$. Since for any $1 \leq b \leq a$, $\varphi_e(\bar{x}, b-1) = \varphi_e(\bar{x}, b)$ we have $\varphi_e(\bar{x}, 0) = \varphi_e(\bar{x}, a) + a = a$ and $\varphi(e_0, \bar{x}, a) \downarrow$, which completes the proof. $\square$

As a simple application we see for example that a function on ω is semirecursive in $\mathbf{E}$ iff its graph is Π_1^1 (see 5.3). Similarly for $\mathbf{E}^\#$.

The basic idea of proving selection theorems in order to establish structure results is due to GANDY [1967].

RECURSION IN HIGHER TYPES

10. The type structure over ω

10.1. For each integer j , define the set $T^{(j)}$ of *objects of type j* (over ω) by the induction

$$T^{(0)} = \omega$$

$$T^{(j+1)} = \text{the set of all total functions from } T^{(j)} \text{ into } \omega.$$

We will often use superscripted variables $\alpha^j, \beta^j, \gamma^j$ over $T^{(j)}$ to indicate the type, when it is not clear from the context. The members of

$$T = \bigcup_j T^{(j)}$$

are the objects of *higher type* over ω .

A *point* is a finite sequence $x = (x_1 \cdots x_n)$ of objects of higher type; the *type* of $(x_1 \cdots x_n)$ is the maximum of the types of the x_i 's. The *concatenation* of two points $x = (x_1 \cdots x_n)$, $y = (y_1 \cdots y_m)$ is the point

$$x^\frown y = x, y = (x_1 \cdots x_n, y_1 \cdots y_m).$$

We will study recursion in higher types by applying the general theory developed so far to the set

$$A = T^* = \text{set of all points,}$$

relative to some appropriate classes of functionals on T^* . As usual, we will identify the one element sequence (α^j) with α^j itself so that we have $T \subseteq T^*$; in particular $\omega \subseteq T^*$.

Moreover, every product of the form

$$\mathcal{X} = T^{(i_1)} \times \cdots \times T^{(i_n)}$$

is also contained in T^* , so we can think of partial functions

$$f: \mathcal{X} \rightarrow \omega$$

as partial functions on T^* whose domain is contained in $\mathcal{X}$. We are ultimately interested in studying recursive partial functions on these *spaces*. By definition, if $\mathcal{X} = X_1 \times \cdots \times X_n$ and $\mathcal{Y} = Y_1 \times \cdots \times Y_m$, then

$$\mathcal{X} \times \mathcal{Y} = X_1 \times \cdots \times X_n \times Y_1 \times \cdots \times Y_m,$$

so the collection of these spaces contained in T^* is closed under cartesian products.

10.2. We will need some simple mappings which embed $T^{(j)}$ into $T^{(k)}$ when $j \leq k$ (type increasing functions) and their inverses (type decreasing functions). Put first

$$u^1(n) = \lambda m(n), \quad d_0(\alpha^1) = \alpha^1(0);$$

clearly,

$$u^1: T^{(0)} \rightarrow T^{(1)}, \quad d_0: T^{(1)} \rightarrow T^{(0)},$$

u^1 is one-to-one and for all n ,

$$d_0(u^1(n)) = n.$$

Now, by induction, let

$$u^{j+2}(\alpha^{j+1}) = \lambda \beta^{j+1} \alpha^{j+1}(d_j(\beta^{j+1})),$$

$$d_{j+1}(\alpha^{j+2}) = \lambda \beta^j \alpha^{j+2}(u^{j+1}(\beta^j))$$

and verify easily that u^{j+2} is an injection of $T^{(j+1)}$ into $T^{(j+2)}$ and for all $\alpha^{j+1} \in T^{(j+1)}$

$$d_{j+1}(u^{j+2}(\alpha^{j+1})) = \alpha^{j+1}.$$

Mappings

$$u^{j,k} : T^{(j)} \rightarrow T^{(k)} \quad (j < k),$$

$$d_{j,k} : T^{(k)} \rightarrow T^{(j)} \quad (j < k)$$

are defined easily by iterating these, i.e.,

$$u^{j,j+1} = u^{j+1}, \quad d_{j,j+1} = d_j,$$

$$u^{j,j+2} = u^{j+2} \circ u^{j+1}, \quad d_{j,j+2} = d_j \circ d_{j+1},$$

etc. It is also convenient to let

$$u^{j,j} = d_{j,j} = \text{the identity on } T^{(j)}.$$

Now all the $u^{j,k}$ are one-to-one and $d_{j,k}(u^{j,k}(\alpha^j)) = \alpha^j$, ($j \leq k$, $\alpha^j \in T^{(j)}$).

11. Kleene classes of functionals on T^*

We now come to the main notions which underlie recursion theory in higher types.

11.1. DEFINITION. A class $\mathcal{K}$ of functionals on $A = T^*$ is a *Kleene class* if it is suitable, contains the functions (i)–(iii) and is closed under the rules (iv), (v) below. We use variables $x, y, z, \dots$ for members of T^* and σ, τ for finite sequences of members of T^* (including the empty sequence).

(i) *Type specifying function*:

$$\chi(j, x) = \begin{cases} 0 & \text{if } j \in \omega, x \in T^{(j)}, \\ 1 & \text{otherwise.} \end{cases}$$

(ii) *Length function*:

$$\text{length}(x) = n \quad \text{if } x = (x_1 \cdots x_n).$$

(iii) *Application of type 1 objects*:

$$\varphi(x, n) = \begin{cases} x(n) & \text{if } x \in T^{(1)}, n \in \omega, \\ 0 & \text{otherwise.} \end{cases}$$

(iv) *Application of type > 1 objects*: If $\Phi(x, y, \sigma, \bar{f})$ is in $\mathcal{K}$, then for each j

$$\Psi_i(y, \sigma, \bar{f}) = \Psi(y, \sigma, \bar{f}) = \begin{cases} y(\lambda\alpha'\Phi(\alpha^i, y, \sigma, \bar{f})) & \text{if } y \in T^{(j+2)}, \\ 0 & \text{if } y \notin T^{(j+2)}, \end{cases}$$

is also in $\mathcal{K}$. It is understood here that if $y \in T^{(j+2)}$, then $\Psi(y, \sigma, \bar{f})$ is undefined unless $\lambda\alpha'\Phi(\alpha^i, y, \sigma, \bar{f})$ is total.

(v) *Substitutions by concatenation and point projection*: Recall that the concatenation mapping is the total mapping (from $T^* \times T^*$ into T^*)

$$t(x, y) = x^\frown y = x, y.$$

Point projection is the total mapping from $T^* \times T^*$ into T^* given by

$$p(x, i) = \begin{cases} x_i & \text{if } x = (x_0 \cdots x_{n-1}), i \in \omega \text{ \& } i < n, \\ 0 & \text{otherwise.} \end{cases}$$

Using (iii) and (iv) we can prove by induction on $j \geq 1$ that

$$\varphi_j(x, y) = \begin{cases} x(y) & \text{if } x \in T^{(j)}, y \in T^{(j-1)}, \\ 0 & \text{otherwise,} \end{cases}$$

is also in $\mathcal{K}$.

Suppose now $\mathcal{K}$ is a Kleene class and

$$\varphi : \mathcal{X} \rightarrow \omega$$

is a partial function on some space $\mathcal{X} = X_1 \times \cdots \times X_n \subseteq T^*$. We say that φ is $\mathcal{K}$ -recursive if it is $\mathcal{K}$ -recursive (in the sense of 2.2) when we consider it as a partial function on T^* whose domain happens to be included in $\mathcal{X}$; this is easily equivalent to saying that there is a $\mathcal{K}$ -recursive $\varphi^* : T^* \rightarrow \omega$ whose restriction to $\mathcal{X}$ is φ . By the definitions, this means that there is an operative functional $\Phi(\sigma, x, f)$ in $\mathcal{K}$ and integers $n_1, \dots, n_k$ such that

$$\varphi(x) = \Phi^\infty(n_1, \dots, n_k, x) \quad (x \in \mathcal{X}).$$

These partial functions are the main objects of our study.

It is also natural to call a partial mapping

$$\theta : \mathcal{X} \rightarrow T^{(j+1)}$$

$\mathcal{K}$ -recursive if there is a $\mathcal{K}$ -recursive partial function

$$\varphi : T^{(j)} \times \mathcal{X} \rightarrow \omega$$

such that

$$\theta(x) = \lambda\alpha'\varphi(\alpha^j, x);$$

similarly,

$$\theta : \mathcal{X} \rightarrow \mathcal{Y} = T^{(i_1)} \times \dots \times T^{(i_n)}$$

is $\mathcal{K}$ -recursive if

$$\theta(x) = (\theta_1(x) \cdots \theta_n(x)),$$

with $\mathcal{K}$ -recursive $\theta_1, \dots, \theta_n$.

11.2. Let $\mathcal{K}_0$ be the smallest Kleene class on T^* . More generally, given a finite list of functionals $\bar{\Phi} = (\Phi_1 \cdots \Phi_n)$ on T^* , let $\mathcal{K}_0[\bar{\Phi}]$ be the smallest Kleene class of functionals which contains $\Phi_1 \cdots \Phi_n$. Instead of $\mathcal{K}_0$ -recursive we say *Kleene recursive* and instead of $\mathcal{K}_0[\bar{\Phi}]$ -recursive we say *Kleene recursive in $\bar{\Phi}$* .

For example the mappings $u^{j,k}, d_{j,k}$ given in 10.2 are all Kleene recursive.

12. Kleene recursion relative to objects of higher type and quantifiers

To illustrate the basic notions, let us consider now some interesting examples of higher type recursion. Our discussion here parallels that in Sections 4 and 5.

12.1. Every object

$$F = {}^j F \in T^{(j)} \quad (j \geq 1)$$

of higher type can be viewed as a functional on T^* , where for $j \geq 2$

$$F(f) = \begin{cases} F(f \upharpoonright T^{(j-2)}) & \text{if } f \upharpoonright T^{(j-2)} \text{ is total,} \\ \text{undefined} & \text{otherwise,} \end{cases}$$

and for $j = 1$,

$$F(x) = \begin{cases} F(x) & \text{if } x \in \omega, \\ 0 & \text{if } x \notin \omega. \end{cases}$$

Thus we can study *recursion relative to a fixed higher type object F* , i.e., $\mathcal{K}_0[F]$ -recursion. Of particular importance are the objects ${}^j E$ ($j \geq 2$) which embody existential quantification over $T^{(j-2)}$,

$${}^j E(\alpha^{j-1}) = \begin{cases} 0 & \text{if } \exists \alpha^{j-2} (\alpha^{j-1}(\alpha^{j-2}) = 0), \\ 1 & \text{if } \forall \alpha^{j-2} (\alpha^{j-1}(\alpha^{j-2}) \neq 0). \end{cases}$$

Our first result here is very useful — it shows that Kleene recursion in a higher type object can be defined in terms of (absolute) Kleene recursion by substitution.

12.2. THEOREM (KLEENE [1959]). *Let $F = {}^1F$ be an object of type $j \geq 1$. A partial function $\varphi : \mathcal{X} \rightarrow \omega$ is Kleene recursive in F if and only if there is a Kleene recursive partial function $\psi : T^{(j)} \times \mathcal{X} \rightarrow \omega$ such that for all $x \in \mathcal{X}$,*

$$\varphi(x) = \psi(F, x).$$

PROOF In one direction it is enough to associate with each $\Phi(\sigma, y, \sigma', g)$ in $\mathcal{K}_0$ a functional $\Phi^*(\sigma, \sigma', f, g)$ in $\mathcal{K}_0[F]$ such that

$$\Phi(\sigma, F, \sigma', g) = \Phi^*(\sigma, \sigma', \lambda\tau\tau'g(\tau, F, \tau'), g).$$

Because then if Φ is operative we can easily prove by induction on ξ that $\Phi^\xi(\sigma, F, \sigma') = w \Rightarrow \Phi^{*\xi}(\sigma, \sigma', \Phi^\infty) = w$ and $\Phi^{*\xi}(\sigma, \sigma', \Phi^\infty) = w \Rightarrow \Phi^\infty(\sigma, F, \sigma') = w$ so that $\Phi^\infty(\sigma, F, \sigma') = \Phi^{*\infty}(\sigma, \sigma', \Phi^\infty)$ and hence $\Phi^\infty(\sigma, F, \sigma')$ is recursive in F . The construction of Φ^* is by induction on the construction of $\mathcal{K}_0$ and it is straightforward. For example, if

$$\Phi(\sigma, y, \sigma', g) = g(\sigma, y, \sigma')$$

we take

$$\Phi^*(\sigma, \sigma', f, g) = f(\sigma, \sigma')$$

while if

$$\Phi(\sigma, y, \sigma', g) = g(\sigma, \sigma')$$

(so that y does not appear in g) we put

$$\Phi^*(\sigma, y, \sigma', f, g) = g(\sigma, \sigma').$$

On the other hand if (as in 11.1(v))

$$\Psi(\sigma, y, \sigma', g) = y(\lambda\alpha^{j-2}\Phi(\alpha^{j-2}, \sigma, y, \sigma', g))$$

we let

$$\Psi^*(\sigma, \sigma', f, g) = F(\lambda z\Phi^*(z, \sigma, \sigma', f, g)).$$

For the converse, we prove that if $\Phi(\sigma, f)$ is a functional in $\mathcal{K}_0[F]$, then there is a functional $\Phi^*(y, \sigma, g)$ in $\mathcal{K}_0$ such that

$$\Phi(\sigma, \lambda\tau g(F, \tau)) = \Phi^*(F, \sigma, g).$$

Then for operative Φ , we have by induction on ξ that $\Phi^\xi(\sigma) = \Phi^{*\xi}(F, \sigma)$, so $\Phi^\infty(\sigma) = \Phi^{*\infty}(F, \sigma)$ and we are done. The construction of Φ^* is again by induction on the construction of $\mathcal{K}_0[F]$. The only interesting case is when $\Phi = F$; then we take

$$\Phi^*(y, g) = \begin{cases} y(\lambda\alpha^{j-2}g(y, \alpha^{j-2})) & \text{if } y \in T^j, \\ 0 & \text{if } y \notin T^{(j)}, \end{cases}$$

provided $j \geq 2$. If $j = 1$,

$$\Phi^*(y, x) = \begin{cases} y(x) & \text{if } y \in T^{(1)}, x \in \omega, \\ 0 & \text{otherwise.} \end{cases} \quad \square$$

12.3. Given a quantifier Q on some $T^{(j)}$, we associate with it the object of type $j + 2$

$${}^{j+2}F_Q(\alpha^{j+1}) = \begin{cases} 0 & \text{if } Q\alpha^j (\alpha^{j+1}(\alpha^j) = 0), \\ 1 & \text{if } \check{Q}\alpha^j (\alpha^{j+1}(\alpha^j) \neq 0), \end{cases}$$

and the functional on T^*

$${}^{j+2}F_Q^*(f) = \begin{cases} 0 & \text{if } Q\alpha^j (f(\alpha^j) = 0), \\ 1 & \text{if } \check{Q}\alpha^j (f(\alpha^j) \neq 0), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

In particular if $Q = \exists'$ is the existential quantifier on the objects of type j , we get ${}^{j+2}E$ and ${}^{j+2}E^*$ respectively. As in 5.4, ${}^{j+2}F_Q$ is easily Kleene recursive in ${}^{j+2}F_Q^*$, ${}^{j+2}E^*$.

12.4. We are mainly interested in studying Kleene recursion relative to functionals which concentrate (in the sense of 4.1) on

$$T_m^* = \text{set of all points type } \leq m,$$

for some m . These surely include all the examples we have introduced.

Suppose $\bar{\Phi} = (\Phi_1 \cdots \Phi_n)$ is a finite list of such functionals. Then it is easy to see that all functionals in $\mathcal{K}_0[\bar{\Phi}]$ concentrate on T_m^* and moreover

$$\mathcal{K}_0[\bar{\Phi}] \upharpoonright T_m^* = \mathcal{K}_0(T_m^*)[\bar{\Phi} \upharpoonright T_m^*],$$

where $\mathcal{K}_0(T_m^*)[\bar{\Psi}]$ is the smallest suitable class of functionals on T_m^* containing all functionals in $\bar{\Psi}$ which also satisfies conditions (i)–(vi) of 11.1 (appropriately restricted to T_m^*).

As in 4.2, we can easily check that if type $(\mathcal{X}) = 0$, then a partial function $f: \mathcal{X} \rightarrow \omega$ is Kleene recursive (or Kleene recursive in some fixed $\alpha \in T^{(1)}$) exactly when it is recursive (or recursive in α) in the sense of ordinary recursion theory. Again, as in 5.3, we can verify that if type $(\mathcal{X}) \leq 1$ and $R \subseteq \mathcal{X}$, then R is Kleene semirecursive in 2E (or ${}^2E^*$) exactly when R is Π_1^1 .

13. Normality and enumeration in higher type recursion

When we study recursion in functionals $\bar{\Phi}$ which concentrate on some T_m^* , we do not expect to have normality on all of T^* in the sense of Section 6. We introduce therefore a simple modification of this notion, which will cover our present situation.

13.1. Let $\mathcal{F}$ be a class of functionals on a set A , let $\omega \subseteq B \subseteq A$ and let Φ be a functional. We say that Φ is *normal in $\mathcal{F}$ on B* if there is an $\mathcal{F}$ -recursive functional Δ_Φ such that $\Phi \upharpoonright B, \Delta_\Phi \upharpoonright B$ satisfy conditions (i) and (ii) of 6.2 (with A replaced by B there). We say that $\mathcal{F}$ is *normal on B* if every $\Phi \in \mathcal{F}$ is normal in $\mathcal{F}$ on B . Analogously to Proposition 6.4 we now have

13.2. PROPOSITION. *Let $\bar{\Phi} = (\Phi_1 \cdots \Phi_n)$ be a finite list of functionals on T^* which concentrate on T_m^* . If each Φ_i is normal in $\mathcal{K}_0[\bar{\Phi}, {}^2E, \dots, {}^mE]$ on T_m^* , then $\mathcal{K}_0[\bar{\Phi}, {}^2E, \dots, {}^mE]$ is normal on T_m^* . (If $m \leq 1$, then we just have $\mathcal{K}_0[\bar{\Phi}]$ above.)*

PROOF. It is similar to the proof of 6.4. We have to consider the additional cases coming from 11.1 of which the only interesting one is 11.1(iv). So consider $\Phi(x, y, \sigma, f)$ and assume we have found Δ_Φ that satisfies 6.2, working on T_m^* of course. Let then j be such that $j+2 \leq m$ and put

$$\Psi(y, \sigma, \bar{f}) = \begin{cases} y(\lambda \alpha^j \Phi(\alpha^j, y, \sigma, \bar{f})) & \text{if } y \in T^{(j+2)}, \\ 0 & \text{otherwise.} \end{cases}$$

Since $\Psi(y, \sigma, \bar{f}) \downarrow \Leftrightarrow \forall \alpha^j (\Phi(\alpha^j, y, \sigma, \bar{f}) \downarrow)$ or $y \notin T^{(j+2)}$, we take

$$\Delta_\Psi(y, \sigma, \bar{f}, \bar{\delta}) = \begin{cases} 1 \div {}^{j+2}E(\lambda \alpha^j (1 \div \Delta_\Phi(\alpha^j, y, \sigma, \bar{f}, \bar{\delta}))) & \text{if } y \in T^{(j+2)}, \\ 0 & \text{if } y \notin T^{(j+2)}. \quad \square \end{cases}$$

Call a finite sequence of functionals $\bar{\Phi}$ *normal* on T_m^* if each functional in $\bar{\Phi}$ is normal in $\mathcal{K}_0[\bar{\Phi}]$ on T_m^* . Noticing that each object $F = {}^{j+2}F$ concentrates on T_j^* , and similarly for quantifiers on $T^{(j)}$ we have the following analog of 6.5:

13.3. THEOREM. (i) *Let $F = {}^{j+2}F$ be an object of type ≥ 2 ; then $F, {}^2E, \dots, {}^{j+2}E$ is normal on T_{j+2}^* .*

(ii) *Let Q be a quantifier on $T^{(j)}$; then $F_Q^*, {}^2E, \dots, {}^{j+2}E$ is normal on T_{j+2}^* .*

We will consider the consequences of normality for the structure of semirecursive relations especially in the case of recursion relative to objects of higher type in Section 17.

We proceed now to prove the enumeration property in the present context. The main fact is the following

13.4. PROPOSITION. *Let $\mathcal{K}$ be a Kleene class of functionals on T^* . Then $\mathcal{K}$ admits a coding of tuples on T^* .*

PROOF. Put

$$\langle x_1 \cdots x_n \rangle = 2^n \cdot 3^{\text{length}(x_1)+1} \cdots p_n^{\text{length}(x_n)+1}, x_1, x_2, \dots, x_n$$

where as usual

$$y, x_1, \dots, x_n = \text{concatenation of } y, x_1, \dots, x_n = y \cap x_1 \cap \cdots \cap x_n.$$

It is routine to check that $\mathcal{K}$ admits this coding. $\square$

It follows from this proposition and 8.4 that for every finite list of functionals $\bar{\Phi}$ on T^* , the class of partial functions on T^* which are Kleene recursive in $\bar{\Phi}$ has the enumeration property. From this in turn and the results of Section 9 we obtain immediately the following theorems.

13.5. ENUMERATION AND $s - m - n$ THEOREM. *For each finite list $\bar{\Phi} = (\Phi_1, \dots, \Phi_n)$ of functionals on T^* and each space $\mathcal{X}$, we can define a partial function*

$$\varphi^{\mathcal{X}} : \omega \times \mathcal{X} \rightarrow \omega,$$

which is Kleene recursive in $\bar{\Phi}$ such that following conditions hold:

(i) *A partial function $\psi : \mathcal{X} \rightarrow \omega$ is Kleene recursive in $\bar{\Phi}$ exactly when for some $e \in \omega$ and all $x \in \mathcal{X}$,*

$$\psi(x) = \varphi_e^{\mathcal{X}}(x) = \varphi^{\mathcal{X}}(e, x)$$

(i.e. each $\varphi^{\mathcal{X}}$ is universal for Kleene recursion in $\bar{\Phi}$, on $\mathcal{X}$).

(ii) *For each space $\mathcal{X}$ of type 0 and each $\mathcal{Y}$ there is a total recursive function*

$$S_{\mathcal{Y}}^{\mathcal{X}} : \omega \times \mathcal{X} \rightarrow \omega$$

such that

$$\varphi^{\mathcal{X} \times \mathcal{Y}}(e, x_1 \cdots x_m, y_1, \dots, y_n) = \varphi^{\mathcal{Y}}(S_{\mathcal{Y}}^{\mathcal{X}}(e, x_1, \dots, x_m), y_1, \dots, y_n).$$

We will call a system of universal partial functions $\{\varphi^{\mathcal{X}}\}$ with these properties *good*

13.6. THE (SECOND) RECURSION THEOREM. *If $\{\varphi^x\}$ is a good universal system, then for each partial function $\psi: \omega \times \mathcal{X} \rightarrow \omega$ which is Kleene recursive in $\bar{\Phi}$, there is some $e \in \omega$ such that*

$$\varphi_e^x(x) = \varphi_e(x) = \psi(e, x).$$

14. The original definition of Kleene

We give in this section the original definition of recursion in higher types given in KLEENE [1959]. In the next section we will establish the equivalence of this original definition with ours.

14.1. In our terminology, Kleene defines a specific operative functional $\Theta(e, x, f)$, where e varies over ω , x varies over T^* and f varies over partial functions on $\omega \times T^*$. Then he calls a partial function $\varphi: \mathcal{X} \rightarrow \omega$ *recursive* if for some fixed $e \in \omega$ (an index for φ) and all $x \in \mathcal{X}$,

$$\varphi(x) = \Theta^\infty(e, x).$$

Thus, in effect, he gives a single *master recursion* and takes as recursive all partial functions (on spaces) reducible to it, instead of specifying the *form* of inductions which are allowed.

The fixed point of Θ is indicated by

$$\{e\}(x) = \Theta^\infty(e, x).$$

It is easier then to describe $\Theta(e, x, f)$ if we write $\{e\}(x)$ for $\Theta(e, x, f)$ in the left of the equations below and again $\{e\}(x)$ for $f(e, x)$ in the right of the same equations. Since Kleene identifies any two points which contain the same objects in the same order within each fixed type (like $(n, \alpha, m, \alpha^2, \beta)$ and $(n, \alpha, \beta, \alpha^2, m)$), we will assume in (i)–(ix) below that all points are in *simplified* form i.e. the objects of type 0 precede those of type 1 etc. Thus an expression like (α^j, x) where x is a simplified point abbreviates the simplified point whose first type j object is α^j and which agrees with x otherwise. Then we let $\{e\}(x) = \{e\}(x^*)$, where x^* is the unique point in simplified form equivalent to x (e.g. $(n, \alpha, m, \alpha^2, \beta)^* = (n, m, \alpha, \beta, \alpha^2)$). The definition is by cases on the form of e as a sequence code and the *arity* of x , where

$$\text{arity}(x) = \langle n_0, n_1, \dots, n_r \rangle,$$

with $r = \text{type}(x)$ and for $0 \leq i \leq r$, n_i = number of type i objects appearing in x :

- (i) $\{e\}(n, x) = n + 1$ if $e = \langle 1, \text{arity}(n, x) \rangle$,
- (ii) $\{e\}(x) = q$ if $e = \langle 2, \text{arity}(x), q \rangle$,
- (iii) $\{e\}(n, x) = n$ if $e = \langle 3, \text{arity}(n, x) \rangle$,
- (iv) $\{e\}(x) = \{e_2\}(\{e_1\}(x), x)$ if $e = \langle 4, \text{arity}(x), e_1, e_2 \rangle$,
- (v) $\{e\}(k, t, l, m, n, x) = \begin{cases} k' & \text{if } m = n \\ l \cdot t & \text{if } m \neq n \end{cases}$ if $e = \langle 5, \text{arity}(k, t, l, m, n, x) \rangle$,
- (vi) $\{e\}(x) = \{e_1\}(x_1)$ if $e = \langle 6, \text{arity}(x), j, k, e_1 \rangle$
- where x_1 contains at least $k + 1$ objects of type j and x comes from x_1 by moving the $(k + 1)$ -st type j object in x_1 to the front of the list,
- (vii) $\{e\}(n, \alpha, x) = \alpha(n)$ if $e = \langle 7, \text{arity}(n, \alpha, x) \rangle$
- (viii) $\{e\}(\alpha^j, x) =$
 $= \alpha^j(\lambda \alpha^{j-2} \{e_1\}(\alpha^j, \alpha^{j-2}, x))$ if $e = \langle 8, \text{arity}(\alpha^j, x), j, e_1 \rangle$ and $j \geq 2$
- (ix) $\{e\}(n, x, y) = \{n\}(x)$ if $e = \langle 9, \text{arity}(n, x, y), \text{arity}(x) \rangle$.

To each e, x such that $\{e\}(x) = \Theta^\infty(e, x)$ is defined we associate as usual the ordinal

$$|e, x| = \text{least } \xi \text{ such that } \Theta^\xi(e, x) \text{ is defined.}$$

14.2. The reader familiar with KLEENE [1959] has certainly noticed that the definition given in 14.1 is not exactly the one given there. The Kleene scheme S5 for introducing primitive recursion has been replaced by an initial function (v). Correspondingly the Kleene indexing is different than the one given in 14.1. It is however well known (and essentially mentioned in KLEENE [1959]) that both ways of presenting the definition are basically the same in the following strong sense: if $\{e\}'(x)$ refers to the KLEENE [1959] variant, then there are total recursive functions $p, q : \omega \rightarrow \omega$ such that $\{e\}(x) = \{p(e)\}'(x)$ and $\{e\}'(x) = \{q(e)\}(x)$. The proof is fairly simple for anyone familiar with KLEENE [1959] and we will omit it. Here we gave a simplified version of the Kleene definition because it is easier to use as a technical tool, which we intend to do in the next section.

14.3. Kleene visualized his inductive definition as leading to a computation procedure for $\{e\}(x)$ which we can explain by an example following KLEENE [1959] (see Fig. 1).

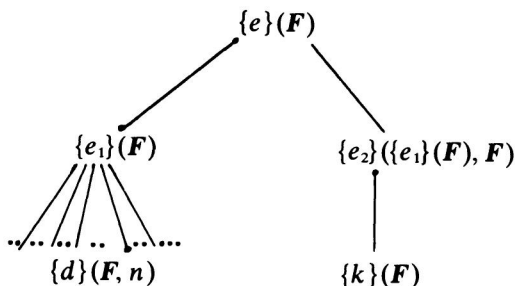


Fig. 1.

Let $e = \langle 4, \langle 0, 0, 1 \rangle, e_1, e_2 \rangle$ and suppose $F = {}^2F$ is a fixed type 2 object. To compute $\{e\}(F)$ we have to compute $\{e_1\}(F)$ and then, if this is defined, $\{e_2\}(\{e_1\}(F), F)$. Say $e_1 = \langle 8, \langle 0, 0, 1 \rangle, 2, d \rangle$. Then to compute $\{e_1\}(F)$ we have to compute $\{d\}(F, n)$ for all $n \in \omega$. Take for example $d = \langle 2, \langle 1, 0, 1 \rangle, 3 \rangle$. Then for all n , $\{d\}(F, n) = 3$. Tracing back the above steps we have that

$$\{e_1\}(F) = F(\lambda n \{d\}(F, n)) = F(\lambda n (3)) = k.$$

So we have to compute now $\{e_2\}(k, F)$. Say $e_2 = \langle 9, \langle 1, 0, 1 \rangle, \langle 0, 0, 1 \rangle \rangle$. Then to compute $\{e_2\}(k, F)$ we must compute $\{k\}(F)$. If this is undefined, so is $\{e\}(F)$. On the other hand if for example $k = \langle 2, \langle 0, 0, 1 \rangle, 5 \rangle$, then $\{k\}(F) = 5$ and tracing these steps back we also have $\{e\}(F) = 5$.

15. Equivalence of the original Kleene definition with ours

It is immediate from the definition in Section 14 that every partial function

$$f: \mathcal{X} \rightarrow \omega$$

which is recursive in the original sense of KLEENE [1959] is also Kleene recursive in our sense of 11.2. We will prove here the converse.

15.1. For each point

$$x \in \mathcal{X} = T^{(u_1)} \times \cdots \times T^{(u_m)},$$

let

$$\text{ch}(x) = \text{ch}(\mathcal{X}) = \langle j_1 \cdots j_m \rangle$$

be the *character* of x and for each finite sequence $\sigma = (x_1, \dots, x_n)$ from T^* let

$$\text{ch}(\sigma) = \langle n, \text{ch}(x_1) \cdots \text{ch}(x_n) \rangle.$$

Let also

$$\hat{\sigma} = x_1, \dots, x_n = x_1 \cap x_2 \cap \cdots \cap x_n$$

= the concatenation of the points $x_1, \dots, x_n$.

Our plan will be to associate with each functional $\Phi(\sigma, f)$ in $\mathcal{K}_0$ a total recursive function $p_\Phi = p : \omega \rightarrow \omega$ such that

$$\Phi^\infty(\sigma) = \{p(\text{ch}(\sigma))\}(\hat{\sigma}).$$

This is of course sufficient, because if $\varphi : \mathcal{X} \rightarrow \omega$ is Kleene recursive in our sense, then for some $\Phi(\tau, x, f) \in \mathcal{K}_0$ we have $\varphi(x) = \Phi^\infty(\bar{n}, x)$, with $\bar{n} \in \omega^k$ so that

$$\varphi(x) = \{e\}(\bar{n}, x)$$

with

$$e = p(\text{ch}(\omega^k \times \mathcal{X})).$$

To define p_Φ we will have to define simultaneously p_Ψ for all (the finitely many) "subfunctionals" Ψ of Φ .

15.2. Notice first that from the definition of a Kleene class we know that a functional of the form $\Phi(\sigma, f)$ is in $\mathcal{K}_0$ if it is one of the functionals (i)–(vii) or is generated according to the rules (viii)–(xii) below (unexplained notation is as in 2.3 and 11.1).

$$(i) \quad \Phi(j, x, \sigma, f) = \begin{cases} 0 & \text{if } j \in \omega, x \in T^{(j)}, \\ 1 & \text{otherwise.} \end{cases}$$

$$(ii) \quad \Phi(x, \sigma, f) = \begin{cases} x & \text{if } x \in \omega, \\ 0 & \text{if } x \notin \omega. \end{cases}$$

$$(iii) \quad \Phi(x, q, f) = \begin{cases} x+1 & \text{if } x \in \omega \\ 0 & \text{if } x \notin \omega. \end{cases}$$

$$(iv) \quad \Phi(x, y, \sigma, f) = \begin{cases} 0 & \text{if } x = y \in \omega, \\ 1 & \text{if } x, y \in \omega, x \neq y, \\ 0 & \text{otherwise.} \end{cases}$$

$$(v) \quad \Phi(\tau, \sigma, f) = f(\tau).$$

$$(vi) \quad \Phi(x, \sigma, f) = \text{length}(x).$$

$$(vii) \quad \Phi(x, y, \sigma, f) = \begin{cases} y(x) & \text{if } y \in T^{(1)}, x \in \omega, \\ 0 & \text{otherwise.} \end{cases}$$

$$(viii) \quad \Psi(\sigma, f) = \Phi(X(\sigma, f), \sigma, f).$$

$$(ix) \quad \Psi(x, \sigma, f) = \begin{cases} \Phi(\sigma, f) & \text{if } x = 0 \\ X(\sigma, f) & \text{if } x \neq 0, x \in \omega, \\ 0 & \text{otherwise.} \end{cases}$$

$$(x) \quad \Psi(y, \sigma, f) = \begin{cases} y(\lambda \alpha^i \Phi(\alpha^i, y, \sigma, f)) & \text{if } y \in T^{(i+2)}, \\ 0 & \text{otherwise.} \end{cases}$$

$$(xi) \quad \Psi(\sigma, f) = \Phi(\pi_1(\sigma) \cdots \pi_k(\sigma), f).$$

$$(xii) \quad \Psi(x, y, \sigma, f) = \Phi(t(x, y), \sigma, f),$$

with t concatenation or point projection.

Define the set $\text{Sub}(\Phi)$ of subfunctionals of $\Phi(\sigma, f)$ as follows:

(a) If Φ comes from (i)–(vii) above, then $\text{sub}(\Phi) = \{\Phi\}$.

(b) If Ψ comes from Φ, X as in (viii)–(xii) above, then $\text{sub}(\Psi) = \{\Psi\} \cup \text{Sub}(\Phi) \cup \text{Sub}(X)$.

Finally let $\Phi < X$ if $\Phi \in \text{Sub}(X)$ & $\Phi \neq X$.

15.3. PROPOSITION. *Let $\Phi(\sigma, f)$ be an operative functional in $\mathcal{K}_0$ and let $\Phi_0 \cdots \Phi_c$ be an enumeration of all its subfunctionals such that if $\Phi_i < \Phi_j$, then $i < j$ and $\Phi_c = \Phi$. There is a total recursive function $p(i, t)$ on ω such that for all $i \leq c$,*

$$\Phi_i(\tau, \Phi^\infty) = \{p(i, \text{ch}(\tau))\}(\tau).$$

PROOF. Let us temporarily call a partial function $\varphi: \mathcal{X} \rightarrow \omega$ *Kleene₀ recursive* if it is recursive in the original sense of Kleene. We will need below two simple facts about Kleene₀ recursion which can be easily established from the definitions (or else see KLEENE [1959]):

(i) If

$$\varphi^*(e, x) = \{e\}(x) \quad (x \in \mathcal{X}),$$

then $\{\varphi^*\}$ is a good system of universal partial functions for Kleene₀ recursion. In particular we have the second recursion theorem for Kleene₀ recursion.

(ii) Every partial function on ω which is recursive in the sense of ordinary recursion theory is also Kleene₀ recursive. The converse is also

true as it follows from 12.4 and the remarks in the beginning of the present section.

We define

$$p(i, t) = \{\hat{p}\}(i, t)$$

by using the second recursion theorem for Kleene₀ recursion. We consider cases according to what Φ_i is.

First put $p(i, t) = 0$, if $i > c$.

For $i \leq c$, the definition of $p(i, t)$ is straightforward except when Φ_i comes from 15.2(v), i.e., evaluation. In the other cases $p(i, t)$ is either an explicitly defined recursive function or it is recursively defined in terms of $p(j, t')$ with $j < i$. For example, in case 15.2(viii) we have

$$\Phi_i(\tau, f) = \Phi_j(\Phi_k(\tau, f), \tau, f),$$

for $j, k < i$. Then we have

$$\begin{aligned} \Phi_i(\tau, \Phi^\infty) &= \Phi_j(\Phi_k(\tau, \Phi^\infty), \tau, \Phi^\infty) \\ &= \{p(j, \text{ch}(0, \tau))\}(\{p(k, \text{ch}(\tau))\}(\hat{\tau}), \hat{\tau}) \\ &= \{\langle 4, \text{arity}(\hat{\tau}), p(k, \text{ch}(\tau)), p(j, \text{ch}(0, \tau)) \rangle\}(\hat{\tau}). \end{aligned}$$

So we take $p(i, t) = \langle 4, q_1(t), p(k, t), p(j, q_2(t)) \rangle$, where q_1, q_2 are recursive such that $q_1(\text{ch}(\tau)) = \text{arity}(\hat{\tau})$, $q_2(\text{ch}(\tau)) = \text{ch}(0, \tau)$.

Assume now Φ_i comes from 15.2(v) and to simplify the notation take σ empty, so that

$$\Phi_i(\tau, f) = f(\tau).$$

Then we have

$$\begin{aligned} \Phi_i(\tau, \Phi^\infty) &= \Phi^\infty(\tau) = \Phi(\tau, \Phi^\infty) \\ &= \Phi_c(\tau, \Phi^\infty) = \{p(c, \text{ch}(\tau))\}(\hat{\tau}). \end{aligned}$$

It would seem reasonable to take $p(i, t) = p(c, t)$, but since $c > i$ we cannot expect to have $p(i, t)$ defined in this manner. If $\hat{p}$ is an index of p , however, we also have

$$\begin{aligned} \{p(c, \text{ch}(\tau))\}(\hat{\tau}) &= \{\{\hat{p}\}(c, \text{ch}(\tau))\}(\hat{\tau}) \\ &= \{\langle 9, \text{arity}(0, \hat{\tau}), \text{arity}(\hat{\tau}) \rangle\}(\{\hat{p}\}(c, \text{ch}(\hat{\tau})), \hat{\tau}) \\ &= \{q(\hat{p}, \text{ch}(\tau))\}(\hat{\tau}), \end{aligned}$$

with a recursive function q which is not hard to compute; put then

$$p(i, t) = q(\hat{p}, t)$$

in this case. The proof will hinge on an additional property of this function q which we will explain below.

By the second recursion theorem for Kleene₀ recursion there is an index $\hat{p}$ such that the function $p(i, t) = \{\hat{p}\}(i, t)$ satisfies all the above requirements. Clearly p is total.

To show that p works we prove first by induction on ξ that

$$\Phi_i(\tau, \Phi^{<\xi}) = w \Rightarrow \{p(i, \text{ch}(\tau))\}(\hat{\tau}) = w.$$

For that within any fixed ξ we will have to use induction on i . We leave the easy details to the reader.

For the other direction, we prove

$$\{p(i, \text{ch}(\tau))\}(\hat{\tau}) = w \Rightarrow \Phi_i(\tau, \Phi^\infty) = w$$

by induction on the ordinal

$$|p(i, \text{ch}(\tau)), \hat{\tau}| = \xi$$

(see 14.1) and for each ξ , by taking cases on i .

The only difficult case is when Φ_i comes from 15.2(v). By the definition of $p(i, \text{ch}(\tau))$ in this case, we have

$$\begin{aligned} \{p(i, \text{ch}(\tau))\}(\hat{\tau}) &= \{q(\hat{p}, \text{ch}(\tau))\}(\hat{\tau}) \\ &= \{p(c, \text{ch}(\tau))\}(\hat{\tau}). \end{aligned}$$

Moreover, any natural choice of the function q has the additional property that it *increases* the ordinal of the computation, i.e.

$$\begin{aligned} |p(i, \text{ch}(\tau)), \hat{\tau}| &= |q(\hat{p}, \text{ch}(\tau)), \hat{\tau}| \\ &\geq |\langle 9, \text{arity}(0, \hat{\tau}), \text{arity}(\hat{\tau}) \rangle, p(c, \text{ch}(\tau)), \hat{\tau}| \\ &> |p(c, \text{ch}(\tau)), \hat{\tau}|; \end{aligned}$$

this needs checking, but it is not hard and it is the key to this part of the proof. It allows us to use the induction hypothesis, by which

$$\Phi_c(\tau, \Phi^\infty) = w,$$

so that also

$$\Phi_i(\tau, \Phi^\infty) = \Phi_c(\tau, \Phi^\infty) = w. \quad \square$$

16. The Substitution Theorems of Kleene

16.1. Let $\varphi(y, z)$ be a Kleene recursive partial function and let $\theta : \mathcal{X} \rightarrow \mathcal{Y}$ be a Kleene recursive partial mapping in the sense of 11.1. We consider the question whether

$$\chi(x, z) = \varphi(\theta(x), z)$$

is Kleene recursive. We can assume without loss of generality that $\mathcal{Y} = T^{(0+1)}$, so that

$$\chi(x, z) = \varphi(\lambda \alpha^i \psi(\alpha^i, x), z)$$

for some Kleene recursive partial function ψ .

A counterexample of KLEENE [1959] shows that one cannot expect χ to be Kleene recursive when $j > 0$, even if θ is total. Indeed, let $T(m, n)$ be a recursive relation on ω such that $\forall n T(m, n)$ is not semirecursive (i.e. recursively enumerable). Let

$$\varphi'(\alpha^2, n, m) = \begin{cases} 0 & \text{if } T(m, n), \\ \text{undefined} & \text{if } \neg T(m, n), \end{cases}$$

and let

$$\varphi(\alpha^2, m) = \alpha^2(\lambda n \varphi'(\alpha^2, n, m)).$$

Then φ is Kleene recursive. Let

$$\theta : \omega \rightarrow T^{(2)}$$

be any Kleene recursive *total* mapping. Then

$$\varphi(\theta(0), m)$$

cannot be Kleene recursive since it would then be recursive (in the sense of ordinary recursion theory) so

$$P(m) \Leftrightarrow \varphi(\theta(0), m) \downarrow \Leftrightarrow \forall n T(m, n),$$

would be semirecursive, which it is not.

The following partial substitution theorem is very important.

16.2. THEOREM (KLEENE [1959]). *Let $\varphi : \mathcal{Y} \times \mathcal{Z} \rightarrow \omega$ be a Kleene recursive partial function, let $\theta : \mathcal{X} \rightarrow \mathcal{Y}$ be a Kleene recursive partial mapping and put*

$$\chi(x, z) = \varphi(\theta(x), z);$$

then χ has a Kleene recursive extension.

In more detail, there exists a Kleene recursive partial function $\chi^(x, z)$, such that if $\theta(x)$ and $\varphi(\theta(x), z)$ are both defined, then $\chi^*(x, z)$ is defined and*

$$\chi^*(x, z) = \varphi(\theta(x), z).$$

In particular, if both φ and θ are total, then χ is Kleene recursive.

PROOF (Outline). It is enough to assume that $\mathcal{Y} = T^{(j+1)}$ so that

$$\chi(x, z) = \varphi(\lambda\alpha^j\psi(\alpha^j, x), z).$$

The proof is a typical example of the “index transfer method” which we also used in establishing 15.3. In these arguments, one of the most important steps is to formulate the desired result in a strong form which admits proof by “effective transfinite induction”. In this case, we will associate with each j a recursive function $p_j(e_1, e_2, t)$ such that for each pair of codes e_1, e_2 and points x, y, z

$$(*) \quad \{e_1\}(y, \lambda\alpha^j\{e_2\}(\alpha^j, x, y, z), z) = \{p_j(e_1, e_2, \text{ch}(x, y, z))\}(x, y, z),$$

whenever the left-hand side is defined.

The construction of p_j is by induction on j , so fix some $j > 0$ and assume that $p_0, \dots, p_{j-1}$ have been defined and $(*)$ holds for each of them. (The construction of p_0 is similar to that of p_j ($j > 0$) and we will omit it.)

We will define

$$p(e_1, e_2, t) = p_j(e_1, e_2, t)$$

using the recursion theorem, in terms of its index $\hat{p}$. The definition is by cases on the index e_1 , corresponding to 14.1(i)–(ix). All the cases except (viii), (ix) are straightforward since in them one defines $p(e_1, e_2, t)$ explicitly (and recursively) either absolutely or in terms of $p(e'_1, e'_2, t')$ with $e'_1 < e_1$.

Take now case 14.1(viii). If $t = \text{ch}(x, y, z)$ for points x, y, z with y containing some type $j+1$ object, the definition of $p(e_1, e_2, t)$ is again straightforward. Otherwise we can incorporate y, z in a new sequence so that without any loss of generality we can assume that y is empty and

$$e_1 = (8, \text{arity}(\alpha^{j+1}, z), j+1, (e_1)_3)$$

so that

$$\{e_1\}(\alpha^{j+1}, z) = \alpha^{j+1}(\lambda\alpha^{j-1}\{(e_1)_3\}(\alpha^{j+1}, \alpha^{j-1}, z)).$$

Fix x and z and let

$$\beta^{j+1} = \lambda\alpha^j\{e_2\}(\alpha^j, x, z);$$

then easily

$$\{e_1\}(\beta^{j+1}, z) = \{e_2\}(\lambda\alpha^{j-1}\{(e_1)_3\}(\beta^{j+1}, \alpha^{j-1}, z), x, z).$$

Now

$$\beta^{j+1} = \lambda\alpha^j\{q(e_2)\}(\alpha^j, x, \alpha^{j-1}, z)$$

with a recursive q , so that

$$\begin{aligned} \{(e_1)_3\}(\beta^{j+1}, \alpha^{j-1}, z) &= \{(e_1)_3\}(\lambda\alpha^j\{q(e_2)\}(\alpha^j, x, \alpha^{j-1}, z), \alpha^{j-1}, z) \\ &= \{p((e_1)_3, q(e_2), \text{ch}(x, \alpha^{j-1}, z))\}(x, \alpha^{j-1}, z) \end{aligned}$$

assuming that p is defined and has the required properties on $(e_1)_3, q(e_2), \text{ch}(x, \alpha^{j-1}, z)$; we will argue this when we come to proving that our definition works, but notice that $|(e_1)_3, \lambda\alpha^j\{q(e_2)\}(\alpha^j, x, \alpha^{j-1}, z), \alpha^{j-1}, z| < |e_1, \beta^{j+1}, z|$.

To simplify notation, let

$$d = p((e_1)_3, q(e_2), \text{ch}(x, \alpha^{j-1}, z)),$$

so that we have

$$\{e_1\}(\beta^{j+1}, z) = \{e_2\}(\lambda\alpha^{j-1}\{d\}(x, \alpha^{j-1}, z), x, z).$$

At this point we have reduced the problem of computing $\{e_1\}(\beta^{j+1}, z)$ to a lower type substitution, i.e. plugging $\lambda\alpha^{j-1}\{d\}(x, \alpha^{j-1}, z)$ into $\{e_2\}(\alpha^j, x, z)$. This is not quite in the right form to apply p_{j-1} , but introducing a recursive r (as we did with q above), we let

$$\{d\}(x, \alpha^{j-1}, z) = \{r(d)\}(\alpha^{j-1}, x, z)$$

and we have

$$\begin{aligned} \{e_1\}(\beta^{j+1}, z) &= \{e_2\}(\lambda\alpha^{j-1}\{r(d)\}(\alpha^{j-1}, x, z), x, z) \\ &= \{p_{j-1}(e_2, r(d), \text{ch}(x, z))\}(x, z). \end{aligned}$$

Finally we set

$$p(e_1, e_2, t) = p_{j-1}(e_2, r(d), \text{ch}(x, z)),$$

where clearly $\text{ch}(x, z) = t$.

In Case 14.1(ix) we defined $p(e_1, e_2, t)$ in terms of an index $\hat{p}$ of p as in the proof of 15.3. We omit the details.

The proof that p is total is exactly as in 15.3.

To show that p satisfies (*), one checks by induction on

$$|e_1, y, \lambda\alpha^j\{e_2\}(\alpha^j, x, y, z), z| = \xi$$

and within each ξ by taking cases on e_1 , that

$$(**) \{e_1\}(y, \lambda\alpha^j\{e_2\}(\alpha^j, x, y, z), z) = w \Rightarrow \{p(e_1, e_2, \text{ch}(x, y, z))\}(x, y, z) = w.$$

Again the only difficult case is 14.1(viii) and the argument in that case can be extracted easily from the analysis we made above. $\square$

One cannot prove the converse of (**) for $j > 0$, even assuming that $\lambda\alpha^j\{e_2\}(\alpha^j, x, y, z)$ is total, because of the counterexample we gave in 16.1. For $j = 0$, however, one can verify that

$$\{p(e_1, e_2, \text{ch}(x, y, z))\}(x, y, z) = w \Rightarrow \{e_1\}(y, \lambda n\{e_2\}(n, x, y, z), z) = w$$

by induction on $|p(e_1, e_2, \text{ch}(x, y, z)), x, y, z|$, so that we have:

16.3. THEOREM (KLEENE [1959]). *If $\text{type } (\mathcal{Y}) = 1$, $\varphi : \mathcal{Y} \times \mathcal{Z} \rightarrow \omega$ is a Kleene recursive partial function and $\theta : \mathcal{X} \rightarrow \mathcal{Y}$ is a Kleene recursive partial mapping, then there is a Kleene recursive $\chi^*(x, z)$ such that whenever $\theta(x)$ is defined,*

$$\chi^*(x, z) = \varphi(\theta(x), z).$$

In particular, if θ is total, then $\varphi(\theta(x), z)$ is Kleene recursive.

Again, by a counterexample similar to the one in 16.1 one can see that the hypothesis that $\theta(x)$ is defined is needed above.

Our final result in this section shows that full substitution as in 16.3 is permissible on any type provided an object of sufficiently high type is present. This fact will be quite useful in the sequel.

16.4. THEOREM (Kleene). *Let $\varphi : \mathcal{Y} \times \mathcal{Z} \rightarrow \omega$ be a Kleene recursive partial function, let $\theta : \mathcal{X} \rightarrow \mathcal{Y}$ be a Kleene recursive partial mapping and put*

$$\chi(x, z) = \varphi(\theta(x), z).$$

For each $m \geq \text{type}(\mathcal{Y})$, there is a Kleene recursive partial function $\chi^(\alpha^m, x, z)$ such that for all objects α^m of type m and all x such that $\theta(x)$ is defined, we have*

$$\chi(x, z) = \chi^*(\alpha^m, x, z).$$

In particular, if θ is total, then χ is recursive in every object of type $\geq \text{type}(\mathcal{Y})$.

PROOF (Outline). Assume without loss of generality that $\mathcal{Y} = T^{(j+1)}$, so that $\theta(x) = \lambda \alpha^j \psi(\alpha^j, x)$. Consider first the case when $m = j + 1$.

Using the "index transfer method" again we show that there is a total recursive function p such that if $\lambda \alpha^j \psi(\alpha^j, x)$ is total, then for each α^m

$$(*) \quad \{e\}(y, \lambda \alpha^j \psi(\alpha^j, x), z) = \{p(e, \text{ch}(x, y, z))\}(\alpha^m, x, y, z).$$

The definition of p follows the same pattern as in the proof of 16.2, but we do not need induction on j since we can now use 16.2.

As in the proof of that result, consider only the interesting subcase of case 14.1(viii), when e is such that

$$\{e\}(\lambda \alpha^j \psi(\alpha^j, x), z) = \psi(\lambda \alpha^{j-1} \{(e_1)_3\}(\lambda \alpha^j \psi(\alpha^j, x), \alpha^{j-1}, z), x);$$

if p is defined and has the desired properties on $(e_1)_3$, then this expression is equal to

$$\begin{aligned} \psi(\lambda\alpha^{j-1}\{p((e_1)_3, \text{ch}(\alpha^{j-1}, z, x))\})(\alpha^m, \alpha^{j-1}, z, x, x) = \\ = \psi(\lambda\alpha^{j-1}\{d\})(\alpha^m, \alpha^{j-1}, z, x, x), \end{aligned}$$

where

$$d = p((e_1)_3, \text{ch}(\alpha^{j-1}, z, x)).$$

Using 16.2, we can find a total recursive function h such that

$$(**) \quad \psi(\lambda\alpha^{j-1}\{d\})(\alpha^m, \alpha^{j-1}, z, x, x) = \{h(d, \text{ch}(x, z))\}(\alpha^m, x, z)$$

whenever

$$f = \lambda\alpha^{j-1}\{d\}(\alpha^m, \alpha^{j-1}, z, x)$$

is total and the left-hand side of (**) is defined. It remains only to modify the right-hand side of (**) so that it is defined only when f is a total function and it is here that the presence of the argument α^m is used.

Find a recursive total function h' such that

$$\{h'(d, \text{ch}(x, z))\}(\alpha^m, x, z) = \begin{cases} \{h(d, \text{ch}(x, z))\}(\alpha^m, x, z) & \text{if } \alpha^m(f) \downarrow, \\ \text{undefined} & \text{otherwise} \end{cases}$$

and put in this case

$$p(e, t) = h'(p((e_1)_3, q(t)), t)$$

where q is recursive and such that

$$q(\text{ch}(x, z)) = \text{ch}(\alpha^{j-1}, z, x).$$

Note here that h' can be chosen so that $|h'(d, \text{ch}(x, z)), \alpha^m, x, z| > |d, \alpha^m, \alpha^{j-1}, z, x|$ for all α^{j-1} .

With this definition it is not hard to verify that

$$\{e\}(y, \lambda\alpha^j\psi(\alpha^j, x), z) = w \Rightarrow \{p(e, \text{ch}(x, y, z))\}(\alpha^m, x, y, z) = w$$

by induction on $|e, y, \lambda\alpha^j\psi(\alpha^j, x), z|$ and the converse implication by induction on $|p(e, \text{ch}(x, y, z)), \alpha^m, x, y, z|$, both under the hypothesis that $\lambda\alpha^j\psi(\alpha^j, x)$ is total.

To prove now the general case when

$$m \geq j + 1$$

it is enough to establish the following:

LEMMA. For each Kleene recursive partial function $\varphi(\alpha^j, x)$ the partial function

$$\psi(\alpha^{j+1}, x) = \varphi(d_j(\alpha^{j+1}), x)$$

is also Kleene recursive. (Here d_j is the type decreasing mapping of 10.2.)

PROOF. We use induction on j . For each fixed j we apply again the “index transfer method”. The troublesome case 14.1(viii) is handled easily, noticing that if

$$\varphi(\alpha^j, x) = \alpha^j(\lambda\alpha^{j-2}\chi(\alpha^j, \alpha^{j-2}, x)),$$

then

$$\begin{aligned}\varphi(d_j(\alpha^{j+1}), x) &= d_j(\alpha^{j+1})(\lambda\alpha^{j-2}\chi(\alpha^j, \alpha^{j-2}, x)) \\ &= \alpha^{j+1}(u'(\lambda\alpha^{j-2}\chi(\alpha^j, \alpha^{j-2}, x))) \\ &= \alpha^{j+1}(\lambda\beta^{j-1}\chi(\alpha^j, d_{j-2}(\beta^{j-1}), x))\end{aligned}$$

so that one can easily use the induction hypothesis on j .

This completes the proof of the lemma and our outline of the proof of 16.4. $\square$

16.5. As a simple corollary of those substitution theorems we can now obtain the following facts about relative Kleene recursion. For any two objects F, G , let $F \leq G$ mean that F is Kleene recursive in G , i.e., for some Kleene recursive partial function φ and all α^j ,

$$F(\alpha^j) = \varphi(G, \alpha^j).$$

By 16.2 $\leq$ is a transitive relation. This allows us to define the equivalence relation

$$F \equiv G \Leftrightarrow F \leq G \text{ \& } G \leq F.$$

If $F \equiv G$ we say that F, G have the same *Kleene degree*. If $F \leq G$, then every total function which is Kleene recursive in F is also Kleene recursive in G . This also holds for partial functions (by 16.4) provided only that $\text{type}(F) \leq \text{type}(G)$.

17. Sections and envelopes

17.1. A *pointset* of type $k > 0$ is a subset $R \subseteq \mathcal{X}$ of a space of type $k - 1$. For example, the pointsets of type 1 are the subsets of ω^n , for some n . If $R \subseteq \mathcal{X}$ is a pointset, we write interchangeably

$$x \in R \Leftrightarrow R(x).$$

A *k-pointclass* is a collection of pointsets of type $\leq k$. Given a finite list of functionals $\bar{\Phi}$, the *k-envelope* of $\bar{\Phi}$, in symbols

$${}_k\text{en}(\bar{\Phi}),$$

is the k -pointclass consisting of those pointsets of type $\leq k$ which are Kleene semirecursive in $\bar{\Phi}$, i.e., domains of Kleene recursive in $\bar{\Phi}$ partial functions. The k -section of $\bar{\Phi}$, in symbols

$${}_k\text{sc}(\bar{\Phi}),$$

is the k -pointclass consisting of the pointsets of type $\leq k$ which are Kleene recursive in $\bar{\Phi}$, i.e., their characteristic functions are Kleene recursive in $\bar{\Phi}$. For example, it follows from 12.4 that, for $k = 1, 2$,

$${}_k\text{en}({}^2E) = \text{all } \Pi_1^1 \text{ pointsets of type } \leq k,$$

$${}_k\text{sc}({}^2E) = \text{all } \Delta_1^1 \text{ pointsets of type } \leq k.$$

We will devote the rest of this chapter to the study of properties of envelopes and sections of higher type objects. In general, no interesting results can be stated about the structure of ${}_k\text{en}(\bar{F})$, unless $\bar{F}$ is normal on T_{k-1}^* . By Theorem 13.3(i), if $\bar{F} = (F_1 \cdots F_n)$ and $m = \max\{\text{type}(F_i) : i = 1, \dots, n\} \geq 2$, then $\bar{F}, {}^2E \cdots {}^mE$ is normal on T_m^* , so we will restrict ourselves to the study of ${}_k\text{en}(\bar{F}, {}^2E \cdots {}^mE)$ for $k \leq m + 1$. Note here that ${}^jE \leq {}^mE$, when $j \leq m$ since ${}^jE = d_{j,m}({}^mE)$ (in the notation of 10.2) so that ${}_k\text{en}(\bar{F}, {}^2E \cdots {}^mE) = {}_k\text{en}(\bar{F}, {}^mE)$. Moreover we can code all objects in $\bar{F}$ by a single object G of type m so that ${}_k\text{en}(\bar{F}, {}^mE) = {}_k\text{en}(G, {}^mE)$. This is done by first lifting to type m (using the $u^{j,m}$) all the objects in $\bar{F}$ and then using a simple pairing function for type m objects like $\langle F_1, F_2 \rangle (\alpha^{m-1}) = \langle F_1(\alpha^{m-1}), F_2(\alpha^{m-1}) \rangle$. So from now on we will study

$${}_k\text{en}(F, {}^mE)$$

for $\text{type}(F) = m \geq 2$ and $k \leq m + 1$. We summarize below the basic properties of these envelopes which follow more or less immediately from what we have already proved.

17.2. Let Γ be a k -pointclass. We say that Γ is closed under $\exists^j$ if for each $R \subseteq \mathcal{X} \times T^{(j)}$ in Γ , the pointset

$$P(x) \Leftrightarrow \exists \alpha^j R(x, \alpha^j)$$

is also in Γ . Closure under $\forall^j$ and $\neg, \vee, \wedge$ is defined in the same way. We say that Γ is closed under *substitution by total Kleene recursive mappings* if it contains all the Kleene recursive pointsets of type $\leq k$ and whenever $\theta : \mathcal{X} \rightarrow \mathcal{Y}$ is Kleene recursive and total with $\text{type}(\mathcal{X}), \text{type}(\mathcal{Y}) < k$ and $R(y, z)$ is in Γ , then so is

$$P(x, z) \Leftrightarrow R(\theta(x), z).$$

We say that Γ has the *enumeration property* or is ω -*parametrized* if for each $\mathcal{X}$ of type $\leq k$ there is some $W \subseteq \omega \times \mathcal{X}$ in Γ such that for each $R \subseteq \mathcal{X}$,

$$R \in \Gamma \Leftrightarrow \exists e (R = W_e),$$

where $W_e = \{x: W(e, x)\}$. Finally, we say that Γ is *normed* or has the *prewellordering property* if every $R \in \Gamma$ admits a Γ -norm (see 7.1, for the definition).

We now have the following result whose most important assertion, namely prewellordering and closure under $\exists^0$, are due to GANDY [1967] for $m = 2$, and PLATEK [1966] and MOSCHOVAKIS [1967] for $m \geq 3$ (the proof in MOSCHOVAKIS [1967] is given only for $m = 3$ and GRILLIOT [1967] extended it to all m).

17.3. THEOREM. *Let $F = {}^m F$ be an object of type $m \geq 2$. Let $\Gamma = {}_k \text{en}(F, {}^m E)$, for $1 \leq k \leq m + 1$. Then*

(i) *Γ is closed under total Kleene recursive substitutions, $\wedge$, $\vee$, $\exists^0$, $\forall^j$ ($j \leq m - 2$), is normed and has the enumeration property.*

(ii) *A function $f: \mathcal{X} \rightarrow \omega$, where type $(\mathcal{X}) < k$, is Kleene recursive in $F, {}^m E$ if and only if $\text{graph}(f) \in \Gamma$. In particular a pointset $R \subseteq \mathcal{X}$ of type $\leq k$ is Kleene recursive in $F, {}^m E$ if and only if both R and $\mathcal{X} - R$ are in Γ .*

PROOF. Closure under total Kleene recursive substitution follows from 16.4. Closure under $\wedge$, $\vee$, $\exists^0$ follows from 13.3, 13.4, 9.4 and 7.3. For closure under $\forall^j$ ($j \leq m - 2$) note that if $\varphi(x, \alpha^j)$ is a partial function, then

$$\forall \alpha^j (\varphi(x, \alpha^j) \downarrow) \Leftrightarrow {}^{j+2} E(\lambda \alpha^j \varphi(x, \alpha^j)) \downarrow.$$

Normality and enumeration follow from 13.3 and 13.5. Finally (ii) follows as in 9.4. $\square$

18. Inductive analysis of semirecursive sets

We give here an inductive analysis of the pointsets in ${}_k \text{en}({}^m F, {}^m E)$ which turns out to be the key to many of the further structural properties of envelopes. Some of its immediate applications to the problem of closure of envelopes under higher existential quantification will be given in the next section.

18.1. An operator

$$\Omega : \text{power}(\mathcal{X}) \rightarrow \text{power}(\mathcal{X})$$

on $\mathcal{X}$ is *monotone* if

$$A \subseteq B \subseteq \mathcal{X} \Rightarrow \Omega(A) \subseteq \Omega(B).$$

Given such an operator we define inductively

$$\Omega^\xi = \Omega(\Omega^{<\xi}), \quad \text{where } \Omega^{<\xi} = \bigcup_{\eta < \xi} \Omega^\eta,$$

and we let $\Omega^\infty = \bigcup_\xi \Omega^\xi$ = least fixed point of Ω .

If $R \subseteq \mathcal{X}$, $S \subseteq \mathcal{Y}$ are two pointsets we say that R is *reducible* to S if there is a total Kleene recursive $\theta : \mathcal{X} \rightarrow \mathcal{Y}$ such that $R(x) \Leftrightarrow S(\theta(x))$.

18.2. THEOREM (MOSCHOVAKIS [1967]). *Let $F = {}^m F$ be an object of type $m \geq 2$ and let $m - 1 \leq k \leq m + 1$. Every $P \in {}_k \text{en}(F, {}^m E)$ is reducible to the fixed point Ω^∞ of some monotone operator Ω on a space of type $< k$, which has the form*

$$x \in \Omega(S) \Leftrightarrow \forall y (R(x, y) \Rightarrow y \in S)$$

with $R \in {}_k \text{en}(F, {}^m E)$.

PROOF (outline). To simplify the notation let $G = \langle F, {}^m E \rangle$. Then ${}_k \text{en}(G) = {}_k \text{en}(F, {}^m E)$, so we work with G below. We treat only the case $k = m - 1$ since the other cases are similar and a little easier. It will also be convenient to work with the single standard space $\mathcal{X} = T^{(m-2)}$ of type $m - 2$ and for that we code finite sequences of objects of type $\leq m - 2$ by single objects of type $m - 2$ as follows: If α^j is an object of type $\leq m - 2$ let

$$\tilde{\alpha}^j = u^{j, m-2}(\alpha^j).$$

If $\alpha_0 \cdots \alpha_{n-1}$ is a sequence of objects of type $\leq m - 2$ let

$$\langle \alpha_0 \cdots \alpha_{n-1} \rangle = \lambda \alpha^{m-3} (\langle \tilde{\alpha}_0(\alpha^{m-3}) \cdots \tilde{\alpha}_{n-1}(\alpha^{m-3}) \rangle).$$

The decoding functions are now given as follows: for any object α^{m-2} put

$$(\alpha^{m-2})_i = \lambda \alpha^{m-3} ((\alpha^{m-2}(\alpha^{m-3}))_i)$$

and for any $j \leq m - 2$ let

$$(\alpha^{m-2})^j_i = d_{j, m-2}((\alpha^{m-2})_i).$$

Then, if $j = \text{type}(\alpha_i)$, we have

$$(\langle \alpha_0 \cdots \alpha_{n-1} \rangle)_i = \alpha_i.$$

Clearly all these coding and decoding functions are total Kleene recursive. (The above definitions were given for $m > 2$. We leave to the reader the trivial modifications needed if $m = 2$.) Following KLEENE [1959] and GRILLIOT [1967] let us abbreviate

$$\begin{aligned} \{e\}[\alpha^{m-2}, \alpha^m] = \{e\} & ((\alpha^{m-2})_0^0, \dots, (\alpha^{m-2})_{k_0-1}^0, \dots, (\alpha^{m-2})_{k_0}^1, \dots, \\ & (\alpha^{m-2})_{k_0+k_1-1}^1, \dots, (\alpha^{m-2})_{k_0+\dots+k_{m-3}}^{m-2}, \dots, \\ & (\alpha^{m-2})_{k_0+k_1+\dots+k_{m-2}-1}^{m-2}, \alpha^m), \end{aligned}$$

if e is an index of a partial function having k_i arguments of type $i \leq m-2$ and one argument of type m . It is easy to see that for some Kleene recursive φ ,

$$\{e\}[\alpha^{m-2}, \alpha^m] = \varphi(e, \alpha^{m-2}, \alpha^m).$$

Let

$$W = \{(e, \alpha^{m-2}): \{e\}[\alpha^{m-2}, G] \text{ is defined}\}.$$

It is clearly enough to show that $W = \Omega^\infty$ for an Ω as in the statement of the theorem.

We view each (e, α^{m-2}) as coding the computation $\{e\}[\alpha^{m-2}, G]$ according to the Kleene definition in Section 14. As in 14.3, to compute $\{e\}[\alpha^{m-2}, G]$ we have to compute its subcomputations which all have the form $\{e'\}[\beta^{m-2}, G]$ and therefore are coded by various (e', β^{m-2}) 's. For example, if e is an index and $(e)_0 = 4$ then the subcomputations of (e, α^{m-2}) are $((e)_2, \alpha^{m-2})$ and (letting $l = k_0 + k_1 + \dots + k_{m-3}$)

$$\begin{aligned} & ((e)_3, \langle \{(e)_2\}[\alpha^{m-2}, G], \\ & (\alpha^{m-2})_0^0, \dots, (\alpha^{m-2})_{k_0-1}^0, \dots, (\alpha^{m-2})_l^{m-2}, \dots, (\alpha^{m-2})_{l+k_{m-2}-1}^{m-2} \rangle), \end{aligned}$$

provided that $\{(e)_2\}[\alpha^{m-2}, G]$ is defined.

Put

$R((e, \alpha^{m-2}), (d, \beta^{m-2})) \Leftrightarrow (e \text{ is not an index of the appropriate form and}$

$$e = d \text{ and } \alpha^{m-2} = \beta^{m-2}) \vee ((d, \beta^{m-2}) \text{ is a}$$

subcomputation of $(e, \alpha^{m-2}))$.

Then R is Kleene semirecursive in G . One can see this by noticing that R is defined by cases on what the index e is. In all cases except when $(e)_0 = 4$, R is actually Kleene recursive in G . In case $(e)_0 = 4$ and e accepts the right type of arguments then

$$R((e, \alpha^{m-2}), (d, \beta^{m-2})) \Leftrightarrow$$

$$\Leftrightarrow (d = (e)_2 \ \& \ \beta^{m-2} = \alpha^{m-2}) \vee$$

$$(d = (e)_3 \ \& \ \exists n \{ (e)_2 \} [\alpha^{m-2}, G] = n$$

$$\ \& \ \beta^{m-2} = \langle n, (\alpha^{m-2})_0^0, \dots, (\alpha^{m-2})_{k_0-1}^0, \dots, (\alpha^{m-2})_l^{m-2}, \dots, (\alpha^{m-2})_{l+k_{m-2}-1}^{m-2} \rangle)$$

so it is Kleene semirecursive in G . Now letting

$$(e, \alpha^{m-2}) \in \Omega(S) \Leftrightarrow \forall d, \beta^{m-2} [R((e, \alpha^{m-2}), (d, \beta^{m-2})) \Rightarrow (d, \beta^{m-2}) \in S]$$

we have that $W = \Omega^\infty$ and we are done. $\square$

19. Closure under higher existential quantification

As a simple corollary of the representation theorem in 18.2 we now have:

19.1. THEOREM (MOSCHOVAKIS [1967]). *Let $F = {}^m F$ be an object of type $m \geq 3$. If $R \in {}_{m-1}\text{en}(F, {}^m E)$, then there is some P in ${}_{m-1}\text{en}(F, {}^m E)$ such that*

$$\neg R(x) \Leftrightarrow \exists \alpha^{m-2} P(x, \alpha^{m-2}).$$

PROOF. Let $\theta: \mathcal{X} \rightarrow \mathcal{Y}$ be total Kleene recursive and Ω an operator on $\mathcal{Y}$ as in 18.2 such that $R(x) \Leftrightarrow \Omega^\infty(\theta(x))$. Say

$$y \in \Omega(S) \Leftrightarrow \forall z (Q(y, z) \Rightarrow z \in S),$$

with $Q \in {}_{m-1}\text{en}(F, {}^m E)$. Notice then that

$$\neg \Omega^\infty(y) \Leftrightarrow \exists y_0, y_1, y_2 \dots (y_0 = y \wedge \forall i Q(y_i, y_{i+1})),$$

so that

$$\neg R(x) \Leftrightarrow \exists y_0, y_1 \dots (y_0 = \theta(x) \wedge \forall i Q(y_i, y_{i+1})).$$

To complete the proof we only have to code $y_0, y_1, \dots$ by a single element of $\mathcal{Y}$. For that, assume without loss of generality that $\mathcal{Y} = T^{(m-2)}$ and let

$$\varphi(\alpha^{m-2}, i) = [\alpha^{m-2}]_i = \lambda \alpha^{m-3} \alpha^{m-2} \langle i, \alpha^{m-3} \rangle.$$

Then φ is total Kleene recursive and

$$\neg R(x) \Leftrightarrow \exists \alpha^{m-2} ([\alpha^{m-2}]_0 = \theta(x) \wedge \forall i Q([\alpha^{m-2}]_i, [\alpha^{m-2}]_{i+1})),$$

so we are done. $\square$

The previous result holds as well for $R \in {}_{m+1}\text{en}(F, {}^m E)$ by a modification of the preceding argument (see MOSCHOVAKIS [1967]) but we will have no

use for this stronger version. Notice also that even if $m = 2$, the above proof shows that if for example $R \subseteq \omega$ is in ${}_{1}\text{en}({}^2F, {}^2E)$, then for some $Q(m, n)$ such that $Q \in {}_{1}\text{en}(F, {}^2E)$,

$$\neg R(x) \Leftrightarrow \exists \alpha (\alpha(0) = x \wedge \forall i Q(\alpha(i), \alpha(i+1))).$$

In view of 19.1 we now have:

19.2. COROLLARY (MOSCHOVAKIS [1967]). *Let $F = {}^mF$ be an object of type $m \geq 3$ and let $k \geq m - 1$; then ${}_k\text{en}(F, {}^mE)$ is not closed under $\exists^{m-2}$.*

As an application of 19.1 we see that for any $m \geq 3$ every pointset of type $\leq m - 1$ semirecursive in mE is recursive in ${}^mE^\#$, since ${}_{m-1}\text{en}({}^mE^\#)$ is obviously closed under $\exists^{m-2}$. In particular,

$${}_{m-1}\text{en}({}^mE) \subsetneq {}_{m-1}\text{en}({}^mE^\#) \quad \text{for } m \geq 3.$$

The negative upper bound 19.2 for the problem of closure of envelopes under existential quantification turns out to be optimal in view of the following important result. This was announced in GRILLIOT [1969b] but was first proved correctly in HARRINGTON and MACQUEEN [1976].

19.3. THEOREM (GRILLIOT [1969b], HARRINGTON and MACQUEEN [1976]). *Let $F = {}^mF$ be an object of type $m \geq 2$. Then ${}_{m-1}\text{en}(F, {}^mE)$ is closed under $\exists^l$ for each $l < m - 2$.*

The proof of 19.3 is rather lengthy and will not be given here. One of its basic ingredients is again the use of the representation theorem 18.2.

20. A guide to the literature

We have presented an exposition of the elementary parts of the theory of recursion in higher types. For the reader who wishes to pursue the study of the subject beyond this, we suggest here some further reading. We will try to cover mainly those aspects of higher type recursion that have been introduced in this chapter. This necessarily leaves out some quite interesting topics of current research, for example the theory of continuous objects and functionals.

For the foundations of recursion in higher types the reader should

consult KLEENE [1959, 1963] and PLATEK [1966] as well as GANDY [1967], where the basic concepts of stage comparison and selection are introduced in the subject.

Much of the early work in the theory was concerned with the construction and study of various hierarchies for the sections of higher type objects in the spirit of the hyperarithmetical hierarchy. Relevant references here are KLEENE [1963], TUGUE [1960], GANDY [1967], SHOENFIELD [1968], MOSCHOVAKIS [1967], GRILLIOT [1969a], HINMAN [1969], and more recently WAINER [1974, 1975].

Later on, Sacks initiated a deeper study of sections, concentrating particularly on the effect of the type of an object F on the structure of its sections. He also studied the analogues for Kleene degrees of many well-known problems from the theory of degrees of unsolvability, like Post's problem. References here include SACKS [1971, 1974, 1975] (where the Plus-1 Theorem is proved), MACQUEEN [1972], HARRINGTON [1973], and SACKS [1976]. See also GRILLIOT [1971].

Still later, the study of the structure of envelopes became another important area of research in higher type recursion. To find out about this recent work the reader can consult MOSCHOVAKIS [1974b], HARRINGTON [1973] (where the Plus-2 Theorem is proved), KECHRIS [1973], HARRINGTON and KECHRIS [1975], and NORMANN [1974].

There are few results in the literature about recursion in specific higher type objects, other than those we have already mentioned in this chapter, e.g. F_α , F_α^* for various Q 's. An exception is the *superjump* which has been studied extensively; put

$${}^3S(e, \alpha^2) = \begin{cases} 0 & \text{if } \{e\}(\alpha^2) \downarrow, \\ 1 & \text{if } \{e\}(\alpha^2) \uparrow, \end{cases}$$

(GANDY [1967]). Although ${}^3E \not\leq S$, recursion in S has many interesting features; see GANDY [1967], PLATEK [1971], ACZEL and HINMAN [1974], HARRINGTON [1973, 1974a] where the generalization of the superjump to higher than type 3 is also studied. Lately, in still unpublished work, HARRINGTON [1974b, 1975] has introduced some particularly interesting new examples of normal functionals whose study looks very promising.

Perhaps the most important open problem of the theory is conceptual, namely to relate higher type recursion with other work in the foundations and to find its proper place within definability theory. There are leads in this direction in the papers we have cited above, but the general question is still wide open.

Acknowledgment

The authors are indebted to L. Kirousis and P. Kolaitis for numerous valuable comments and suggestions on an earlier draft of this paper.

References

- ACZEL, P.
 [1970] Representability in some systems of second order arithmetic, *Israel J. Math.*, **8**, 309–328.
- ACZEL, P. and P.G. HINMAN
 [1974] Recursion in the superjump, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 3–41.
- GANDY, R.O.
 [1967] General recursive functionals of finite type and hierarchies of functionals, *Ann. Fac. Sci. Univ. Clermont-Ferrand*, **35**, 5–24.
- GRILLIOT, T.J.
 [1967] Recursive functions of finite higher types, Thesis, Duke University, Durham, NC.
 [1969a] Hierarchies based on objects of finite type, *J. Symbolic Logic* **34**, 177–182.
 [1969b] Selection functions for recursive functionals, *Notre Dame J. Formal Logic*, **X**, 225–234.
 [1971] On effectively discontinuous type-2 objects, *J. Symbolic Logic*, **36**, 245–248.
- HARRINGTON, L.A.
 [1973] Contributions to recursion theory on higher types, Thesis, M.I.T., Cambridge, MA.
 [1974a] The superjump and the first recursively Mahlo ordinal, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 43–52.
 [1974b] The superjump revisited, mimeographed notes.
 [1975] The Kolmogorov *R*-operator and the first non-projectible ordinal, mimeographed notes.
- HARRINGTON, L.A. and A.S. KECHRIS
 [1975] On characterizing Spector Classes, *J. Symbolic Logic*, **40**, 19–24.
- HARRINGTON, L.A. and D. MACQUEEN
 [1976] Selection in abstract recursion theory, *J. Symbolic Logic*, **41**, 153–158.
- HINMAN, P.G.
 [1969] Hierarchies of effective descriptive set theory, *Trans. Am. Math. Soc.*, **142**, 111–140.
- KECHRIS, A.S.
 [1973] The structure of envelopes: A survey of recursion theory in higher types, M.I.T. Logic Seminar notes.
- KLEENE, S.C.
 [1959] Recursive functionals and quantifiers of finite type I, *Trans. Am. Math. Soc.*, **91**, 1–52.
 [1963] Recursive functionals and quantifiers of finite type II, *Trans. Am. Math. Soc.*, **108**, 106–142.
- MACQUEEN, D.
 [1972] Post's problem for recursion in higher types, Thesis, M.I.T., Cambridge, MA.

MOSCHOVAKIS, Y.

[1967] Hyperanalytic predicates, *Trans. Am. Math. Soc.*, **129**, 249–282.

[1974a] *Elementary Induction on Abstract Structures* (North-Holland, Amsterdam).

[1974b] Structural characterizations of classes of relations, in: J.E. Fenstad and P.G. Hinman, editors, *Generalized Recursion Theory* (North-Holland, Amsterdam) pp. 53–79.

[1976] On the basic notions in the theory of induction, in: *Proceedings of the Fifth International Congress for Logic, Methodology and Philosophy of Science*, London, Ontario, 1975 (forthcoming).

NORMANN, D.

[1974] Imbedding of higher type theories, Preprint Series, Vol. 16, Oslo University.

PLATEK, R.

[1966] Foundations of recursion theory, Thesis, Stanford University, Stanford, CA.

[1971] A countable hierarchy for the superjump, in: R.O. Gandy and C.E.M. Yates, editors, *Logic Colloquium '69* (North-Holland, Amsterdam) pp. 257–271.

ROGERS, H. JR.

[1967] *Theory of Recursive Functions and Effective Computability* (McGraw-Hill, New York).

SACKS, G.E.

[1971] Recursion in objects of finite type, in: *Proceedings of the International Congress of Mathematicians* (Gauthiers-Villars, Paris) pp. 251–254.

[1974] The 1-section of a type n object, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 81–93.

[1975] The k -section of a type n object.

[1976] RE Sets Higher up, in: *Proceedings of the Fifth International Congress for Logic, Methodology and Philosophy of Science*, London, Ontario, 1975 (forthcoming).

SHOENFIELD, J.R.

[1968] A hierarchy based on a type-2 object, *Trans. Am. Math. Soc.*, **134**, 103–108.

TUGUÉ, T.

[1960] Predicates recursive in a type-2 object and Kleene hierarchies, *Comment. Math. Univ. St. Paul*, **8**, 97–117.

WAINER, S.

[1974] A hierarchy for the 1-section of any type-two object, *J. Symbolic Logic*, **39**, 88–95.

[1975] Some hierarchies based on higher type quantification, in: *Logic Colloquium '73*, edited by H. Rose and T. Shepherdson (North-Holland, Amsterdam) pp. 305–316.

*An Introduction to Inductive Definitions**

PETER ACZEL

Contents

Introduction	740
1. What are inductive definitions?	741
1.1. Inductive definitions as generalized formal systems	741
1.2. The well-founded part of a relation	743
1.3. Inductive definitions as operators	744
1.4. Concepts of "proof" for monotone induction	747
1.5. Monotone induction and games	748
1.6. Kernels — the dual of an inductive definition	749
1.7. Some examples of induction in classical mathematics	750
2. Induction in recursion theory	750
2.1. Recursively enumerable relations	750
2.2. Π_1^1 relations	752
2.3. Representability	753
3. Classes of inductive definitions	758
3.1. The general framework	758
3.2. Positive existential induction	761
3.3. Positive elementary induction	764
3.4. Relativisation to a non-trivial monotone quantifier	770
3.5. Non-monotone induction	771
3.6. Induction and admissible sets	774
4. Induction in foundations	778
References	780

* Most of this paper was prepared while the author was visiting Caltech, supported by NSF Grant 75-07562.

Introduction

Inductive definitions of sets are often informally presented by giving some rules for generating elements of the set and then adding that an object is to be in the set only if it has been generated according to the rules. An equivalent formulation is to characterise the set as the smallest set closed under the rules.

Of course the basic example of an inductive definition is the one generating the natural numbers. But it has long proved a useful device when presenting the syntax of a formal language. Further examples of its informal use may be found in logic and other branches of mathematics. POST [1943] realised that the finitary inductive definitions used in presenting the syntax of any standard formal system could all be put in a canonical form, and the general class of such inductions could be fruitfully studied in abstraction from any specific formal system. Since then inductive definitions have played an important role in the development of ordinary recursion theory and its generalisations. Recent work has tended to present the theory of inductive definitions in abstraction from the original motivating intuitions. Our aim here is to give an introduction to the subject which will connect the informal examples with the recent formulation in terms of iterations of monotone operators. We have in mind a reader familiar with the concept of a formal system and with the elements of ordinary recursion theory.

Most of our exposition will be concerned with monotone induction and its role in extensions of recursion theory. But in 3.5 we review some of the work on non-monotone induction, and outline there the separate motivation that has led to its development. In Section 4 we briefly consider inductive definitions in a more general context. For a detailed development of the theory of positive induction see MOSCHOVAKIS [1974a]. Several papers on inductive definability may be found in FENSTAD and HINMAN [1974]. These include a survey, GANDY [1974] and the papers AANDERAA [1974], CENZER [1974], and RICHTER and ACZEL [1974]. MOSCHOVAKIS [1976] gives an abstract algebraic approach to the general theory that applies to both monotone and non-monotone induction and also to recursion in higher types.

1. What are inductive definitions?

1.1. Inductive definitions as generalized formal systems

Inductive definitions are used repeatedly when logicians describe the syntax of their languages. For example the terms of a first order language are defined to be the smallest set of expressions containing the variables and constants and closed under the term formation rule:

If $t_1, \dots, t_n$ are terms and f is an n -ary function symbol of the language then the expression $f(t_1, \dots, t_n)$ is a term.

Similarly the formulae of a first order language are defined to be the smallest set of expressions containing the atomic formulae that are closed under the various formulae formation rules for the logical symbols $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\exists x$, $\forall x$.

For our purpose, the most useful example to consider will be the definition of the class of theorems of a formal system. Consider the Hilbert-style system **H** for first order logic used in Chapter A.1. The set $\text{Th}(\mathbf{H})$ of theorems of **H** is there defined in terms of a notion of “proof” for **H**. But $\text{Th}(\mathbf{H})$ may also be characterized as the smallest set of formulae, containing the axioms, that is closed under the rules of inference. Each instance of a rule of inference has the form:

(*) From the premisses θ for $\theta \in X$, infer the conclusion ψ .

In case of modus ponens X consists of two premisses φ and $(\varphi \rightarrow \psi)$. Instances of the generalization rule only have one premiss. It is convenient to consider an axiom scheme as a special form of rule of inference where in each instance the set of premisses is empty. Using this convention the formal system **H** determines a set $\Phi_{\mathbf{H}}$ of pairs (X, ψ) such that (*) is an instance of a rule of inference of **H**. Then $\text{Th}(\mathbf{H})$ is simply the smallest set closed under (*) for $(X, \psi) \in \Phi_{\mathbf{H}}$.

Generalizing we obtain the following definitions.

1.1.1. DEFINITION. (i) A *rule* is a pair (X, x) where X is a set, called the set of *premisses* and x is the *conclusion*. The rule will usually be written $X \rightarrow x$.

(ii) If Φ is a set of rules (also called a *rule set* below), then a set A is Φ -closed if each rule in Φ whose premisses are in A also has its conclusion in A . We shall write $\Phi : X \rightarrow x$ to denote that the rule $X \rightarrow x$ is in Φ . So A is Φ -closed if $\Phi : X \rightarrow x$ & $X \subseteq A$ implies $x \in A$.

(iii) If Φ is a rule set, then $I(\Phi)$, the *set inductively defined by Φ* , is given by $I(\Phi) = \bigcap \{A \mid A \text{ is } \Phi\text{-closed}\}$.

Note. Φ -closed sets exist; e.g. the set of conclusions of rules in Φ . Also, the intersection of any collection of Φ -closed sets is Φ -closed. In particular $I(\Phi)$ is Φ -closed and hence $I(\Phi)$ is the smallest Φ -closed set.

Returning to our example we see that $\text{Th}(\mathbf{H}) = I(\Phi_{\mathbf{H}})$. Similarly, rule sets can easily be found for inductively defining the sets of terms and formulae of a first order language.

Note. What is usually called a rule of inference or formation rule corresponds to what we have called a rule set. It is the instances of rules of inference or formation rules that correspond to what we have called a rule.

Perhaps the most familiar example of an inductive definition in mathematics is the one that characterizes the set of natural numbers $\omega = \{0, 1, 2, \dots\}$ as the smallest set containing 0 and closed under the successor function, i.e., $\omega = I(\Phi_{\omega})$ where Φ_{ω} consists of the rule $0 \rightarrow 0$ and the rules $\{n\} \rightarrow n + 1$ for $n \in \omega$. This characterization justifies the principle of *mathematical induction*: If $\mathcal{P}$ is a property that holds of 0 and holds of $n + 1$ whenever it holds of n , then $\mathcal{P}$ holds for all natural numbers, i.e. $\{n \in \omega \mid \mathcal{P}(n)\}$ is Φ_{ω} -closed implies $\omega \subseteq \{n \in \omega \mid \mathcal{P}(n)\}$.

Generalizing, we see that to each rule set Φ there is a principle of Φ -induction: If $\mathcal{P}$ is a property, such that whenever $\Phi: X \rightarrow x$ and $\forall y \in X \mathcal{P}(y)$ then $\mathcal{P}(x)$, then $\mathcal{P}(a)$ holds for every $a \in I(\Phi)$.

The above principle is the natural tool to use in proving properties of $I(\Phi)$.

1.1.2. EXAMPLE. To show that every theorem of $\mathbf{H}$ is universally valid in every structure, it suffices to show that for each structure $\mathcal{M}$

$$\{\varphi(v_1, \dots, v_n) \mid \mathcal{M} \models \forall v_1 \cdots \forall v_n \varphi(v_1 \cdots v_n)\} \text{ is } \Phi_{\mathbf{H}}\text{-closed.}$$

So far all our inductive definitions have been finitary, in the sense that each rule has only finitely many premisses. For such Φ we can generalize the standard notion of “proof” for formal systems such as $\mathbf{H}$.

1.1.3. DEFINITION. $a_0, \dots, a_n$ is a (finite length) Φ -proof of b if

- (i) $a_n = b$,
- (ii) for all $m \leq n$ there is an $X \subseteq \{a_i \mid i < m\}$ such that $\Phi: X \rightarrow a_m$.

1.1.4. PROPOSITION. For finitary Φ ,

$$I(\Phi) = \{b \mid b \text{ has a } \Phi\text{-proof}\}.$$

To show that every $b \in I(\Phi)$ has a Φ -proof it suffices to show that the right hand side is Φ -closed and use Φ -induction. For the converse direction if $a_0, \dots, a_n$ is a Φ -proof it suffices to show by induction on $m \leq n$ that $a_m \in I(\Phi)$.

1.2. The well-founded part of a relation

Let $<$ be a binary relation on a set A . The well-founded part of $<$ is the set $W(<)$ of $a \in A$ such that there is no infinite descending sequence $a > a_0 > a_1 > \dots$. The relation $<$ is a *well-founded* relation if $A = W(<)$. $W(<)$ can be inductively defined as follows. Let $\Phi_{<}$ be the set of rules $(<a) \rightarrow a$ for $a \in A$, where $(<a) = \{x \in A \mid x < a\}$.

1.2.1. PROPOSITION. $W(<) = I(\Phi_{<})$.

PROOF. To show that $I(\Phi_{<}) \subseteq W(<)$ it suffices to show that $W(<)$ is $\Phi_{<}$ -closed and use $\Phi_{<}$ -induction. So assume $(<a) \subseteq W(<)$. Now if $a > a_0 > a_1 > \dots$, then $a_0 \in (<a) \subseteq W(<)$. But as $a_0 > a_1 > \dots$, $a_0 \notin W(<)$ which gives a contradiction. Hence $a_0 \in W(<)$.

Conversely, to show $W(<) \subseteq I(\Phi_{<})$ let $a \notin I(\Phi_{<})$. We shall find $a > a_0 > a_1 > \dots$ showing that $a \notin W(<)$. As $a \notin I(\Phi_{<})$, then $(<a) \not\subseteq I(\Phi_{<})$. Hence there is an $a_0 < a$ such that $a_0 \notin I(\Phi_{<})$. Repeating we can find $a_1 < a_0$ such that $a_1 \notin I(\Phi_{<})$. Repeating indefinitely we obtain $a > a_0 > a_1 > \dots$. $\square$

Note that a form of the axiom of choice is needed (the axiom of dependent choices).

The principle of $\Phi_{<}$ -induction, becomes, when $<$ is well-founded, the principle of transfinite induction along a well-founded relation. Associated with transfinite induction is the method of definition by transfinite recursion. This enables one to define a unique function f on $W(<)$ so that for $a \in W(<)$, $f(a)$ is defined in terms of $f(x)$ for $x < a$. The uniqueness and existence of such f can be justified by suitable instances of transfinite induction. As an example we may assign to each $a \in W(<)$ an ordinal $|a|_{<}$ so that

$$|a|_{<} = \text{Sup}\{|x|_{<} + 1 \mid x < a\}.$$

The ordinal $|\<|$ of the well-founded part of $<$ is defined as

$$|\<| = \text{Sup}\{|a|_{<} + 1 \mid a \in W(<)\}.$$

An inductive definition can often be rephrased in the form $\Phi_{<}$ for a suitable $<$.

1.2.2. DEFINITION. The rule set Φ is *deterministic* if

$$\Phi : X_1 \rightarrow x \ \& \ \Phi : X_2 \rightarrow x \quad \text{implies} \quad X_1 = X_2.$$

1.2.3. EXAMPLE. $\Phi_{<}$ is always deterministic. So is Φ_{ω} . Also the rule sets defining the terms and formulae of first order logic are.

Note that Φ_H is not deterministic.

Now let Φ be deterministic and let A be the set of conclusions of rules in Φ . For $x, y \in A$ let $x < y$ if $\Phi : X \rightarrow y$ for some set X such that $x \in X$ and $X \subseteq A$. Then $\Phi_{<}$ is the set of rules $X \rightarrow x$ in Φ such that $X \subseteq A$. Hence we get

1.2.4. PROPOSITION. For deterministic Φ ,

$$I(\Phi) = I(\Phi_{<}).$$

For deterministic Φ , functions on $I(\Phi)$ can be defined by recursion on the way objects in $I(\Phi)$ are generated, as in transfinite recursion. An example of this from syntax is the operation of substitution. Given an individual variable v and a term t , the function assigning to each formula $\varphi(v)$ the formula $\varphi(t)$ obtained by substituting t for all free occurrences of v in $\varphi(v)$ is naturally defined by a recursion on the way a formula $\varphi(v)$ is generated.

1.3. Inductive definitions as operators

Let $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$ where $\text{Pow}(A)$ denotes the set of all subsets of A . The operator φ is *monotone* if $X \subseteq Y \subseteq A$ implies $\varphi(X) \subseteq \varphi(Y)$. Given φ let Φ_{φ} be the set of rules $X \rightarrow x$ such that $X \subseteq A$ and $x \in \varphi(X)$. For monotone φ , $X \subseteq A$ is Φ_{φ} -closed just in case $\varphi(X) \subseteq X$. So $I(\Phi_{\varphi}) = \bigcap \{X \subseteq A \mid \varphi(X) \subseteq X\}$. Hence it is natural to extend the terminology concerning inductive definitions to monotone operators φ and we write $I(\varphi)$ for $\bigcap \{X \subseteq A \mid \varphi(X) \subseteq X\}$ and call it the set *inductively defined by φ* . All inductive definitions can be obtained using monotone operators. For if Φ is a rule set on A (i.e. $X \cup \{x\} \subseteq A$ whenever $\Phi : X \rightarrow x$) we may define a monotone operator $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$ by

$$\varphi(Y) = \{x \in A \mid \Phi : X \rightarrow x \text{ for some } X \subseteq Y\} \quad \text{for } Y \subseteq A.$$

Then $Y \subseteq A$ is Φ -closed just in case $\varphi(Y) \subseteq Y$ so that $I(\Phi) = I(\varphi)$.

For monotone operators φ there is a useful alternative characterization of $I(\varphi)$ using transfinite iterations φ^λ of φ for ordinals λ . Define $\varphi^\lambda \subseteq A$ by transfinite recursion on the ordinal λ so that

$$\varphi^\lambda = \bigcup_{\mu < \lambda} \varphi^\mu \cup \varphi \left(\bigcup_{\mu < \lambda} \varphi^\mu \right).$$

Also define $\varphi^\infty = \bigcup_\lambda \varphi^\lambda$ where λ ranges over all ordinals

If we write $\varphi^{<\lambda}$ for $\bigcup_{\mu < \lambda} \varphi^\mu$, then

$$\varphi^\lambda = \varphi^{<\lambda} \cup \varphi(\varphi^{<\lambda}).$$

The sets $\varphi^{<\lambda}$ may be directly defined by the transfinite recursion

$$\varphi^{<\lambda} = \bigcup_{\mu < \lambda} \varphi(\varphi^{<\mu}),$$

or alternatively by

$$\varphi^{<0} = \emptyset, \quad \varphi^{<\lambda+1} = \varphi^{<\lambda} \cup \varphi(\varphi^{<\lambda}),$$

$$\varphi^{<\lambda} = \bigcup_{\mu < \lambda} \varphi^{<\mu} \quad \text{for limit } \lambda.$$

We may then define $\varphi^\lambda = \varphi^{<\lambda+1}$.

Note. The literature often uses the notation φ^λ for what we have called $\varphi^{<\lambda}$. We have adopted the notation initiated in MOSCHOVAKIS [1974a].

Because $X \subseteq I(\varphi)$ implies $\varphi(X) \subseteq I(\varphi)$, a transfinite induction shows that $\varphi^\lambda \subseteq I(\varphi)$ for all ordinals λ . Hence if we let $\varphi^\infty = \bigcup_\lambda \varphi^\lambda$ then $\varphi^\infty \subseteq I(\varphi)$.

As $\mu < \lambda$ implies $\varphi^{<\mu} \subseteq \varphi^{<\lambda} \subseteq A$, and A is a set there must be an ordinal $\bar{\lambda}$ such that $\varphi^{<\bar{\lambda}+1} = \varphi^{<\bar{\lambda}}$. It follows that $\varphi^\lambda = \varphi^{\bar{\lambda}} = \varphi^{<\bar{\lambda}}$ for all $\lambda \geq \bar{\lambda}$ so that $\varphi^\infty = \varphi^{<\bar{\lambda}}$. Hence $\varphi(\varphi^\infty) = \varphi(\varphi^{<\bar{\lambda}}) \subseteq \varphi^{\bar{\lambda}} = \varphi^\infty$. Hence by φ -induction $I(\varphi) \subseteq \varphi^\infty$. Also for monotone φ , $\mu < \lambda$ implies $\varphi(\varphi^{<\mu}) \subseteq \varphi(\varphi^{<\lambda})$ so that $\varphi^{<\lambda} = \bigcup_{\mu < \lambda} \varphi(\varphi^{<\mu}) \subseteq \varphi(\varphi^{<\lambda})$ and hence $\varphi^\lambda = \varphi(\varphi^{<\lambda})$. It follows that $\varphi^\infty = \varphi(\varphi^\infty)$, φ^∞ is a fixed point of φ (in fact the least one). Thus we have proved:

1.3.1. PROPOSITION. *For monotone $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$,*

- (i) $I(\varphi) = \varphi^\infty$, and
- (ii) $I(\varphi)$ is the least fixed point of φ .

The definition of φ^∞ above does not require the operator φ to be monotone. Hence it is natural to extend the notion of an inductive definition to non-monotone operators by calling φ^∞ the *set inductively defined by φ* for any operator $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$. It has turned out, perhaps rather suprisingly, that the theory of non-monotone inductive definitions is as rich and interesting as the theory for monotone operators, even though naturally occurring examples of non-monotone induction are harder to come by. Perhaps their main motivation can be seen in terms of systems of notations for ordinals. Associated with any operator $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$ is a function $| \cdot |_\varphi$ mapping φ^∞ into an initial segment of ordinals, given by

$$|a|_\varphi = \text{least } \lambda \text{ such that } a \in \varphi^\lambda \quad \text{for } a \in \varphi^\infty.$$

Let $|\varphi| = \text{Sup}\{|a|_\varphi + 1 \mid a \in \varphi^\infty\}$. Then φ^∞ is a set of notations for the ordinals $< |\varphi|$ via the mapping $| \cdot |_\varphi : \varphi^\infty \rightarrow |\varphi|$. (Note that we follow the standard convention of identifying an ordinal with its set of predecessors.) The ordinal may also be characterized as the least ordinal $\bar{\lambda}$ such that $\varphi^{\bar{\lambda}} = \varphi^{<\bar{\lambda}}$. Hence $\varphi^\infty = \varphi^{|\varphi|} = \varphi^{<|\varphi|}$.

1.3.2. EXAMPLE. Let $<$ be a binary relation on the set A and let φ be the monotone operator corresponding to the rule set $\Phi_<$, so that $W(<) = I(\varphi) = \varphi^\infty$. Then it is easily seen that $\varphi^\lambda = \{a \in W(<) \mid |a|_\varphi \leq \lambda\}$, so that $|a|_\varphi = |a|_<$ for $a \in W(<)$ and $|\varphi| = |<|$.

An interesting general problem connected with an operator $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$ is to characterize or estimate the ordinal $|\varphi|$. As $| \cdot |_\varphi : \varphi^\infty \rightarrow |\varphi|$ is a surjection and $\varphi^\infty \subseteq A$ the cardinality of $|\varphi|$ must be $\leq$ the cardinality of A .

For monotone operators a better bound can often be found. If κ is a cardinal let us say that φ is κ -based if:

$$x \in \varphi(X) \text{ implies } x \in \varphi(Y) \text{ for some } Y \subseteq X \text{ of cardinality } < \kappa.$$

1.3.3. EXAMPLE. If Φ is a finitary rule set on A , then the monotone operator φ corresponding to it is ω -based. In general if every set of premisses of a rule in Φ has cardinality $< \kappa$, then φ is κ -based.

1.3.4. PROPOSITION. Let φ be a κ -based monotone operator where κ is regular. Then $|\varphi| \leq \kappa$, so that $I(\varphi) = \varphi^\kappa$.

PROOF. It suffices to show that $\varphi^* \subseteq \varphi^{<\kappa}$. So let $x \in \varphi^* = \varphi(\varphi^{<\kappa})$. Then $x \in \varphi(X)$ for some $X \subseteq \varphi^{<\kappa}$ of cardinality $< \kappa$. By the regularity of κ , $X \subseteq \varphi^{<\lambda}$ for some $\lambda < \kappa$, so that $x \in \varphi(\varphi^{<\lambda}) = \varphi^\lambda \subseteq \varphi^{<\kappa}$ as required. $\square$

1.3.5. EXAMPLE. If Φ is a finitary rule set with corresponding monotone operator φ , then $|\varphi| \leq \omega$ and $I(\varphi) = \varphi^{<\omega} = \bigcup_{n < \omega} \varphi^{<n}$ where $\varphi^{<0} = \emptyset$ and $\varphi^{<n+1} = \varphi(\varphi^{<n})$ for $n < \omega$.

1.4. Concepts of “proof” for monotone induction

In 1.1.3 we formulated a notion of finite length proof appropriate for finitary rule sets. We now consider a more general notion.

1.4.1. DEFINITION. Let φ be a monotone operator on A . A transfinite sequence $\{a_\mu\}_{\mu \leq \lambda}$ is a φ -proof of b with length λ if

- (i) $a_\lambda = b$.
- (ii) $a_\nu \in \varphi(\{a_\mu \mid \mu < \nu\})$ for all $\nu \leq \lambda$.

As in Proposition 1.1.4 we get:

1.4.2. PROPOSITION. (i) For any regular cardinal κ , $\varphi^{<\kappa} = \{a \in A \mid a \text{ has a } \varphi\text{-proof of length } < \kappa\}$.

- (ii) $I(\varphi) = \{a \in A \mid a \text{ has a } \varphi\text{-proof}\}$.

It is sometimes convenient to use an alternative notion of proof that uses well-founded trees instead of transfinite sequences. An example is the notion of derivation for the Gentzen style system **G** of Chapter A.1. There the appropriate rule set is finitary so that the well-founded trees are actually finite.

1.4.3. DEFINITION. A (well-founded) tree T is a set of finite sequences of length > 0 such that

- (i) There is exactly one sequence of length one in T . It is called the *root* (a_τ) of the tree.

- (ii) If $(a_1, \dots, a_{n+1}) \in T$, then $(a_1, \dots, a_n) \in T$.

- (iii) T is well-founded in the sense that there is no infinite sequence $a_1, a_2, \dots$ such that $(a_1, \dots, a_n) \in T$ for all $n > 0$. Alternatively, the relation $<_\tau$ is well-founded, where

$$(a_1, \dots, a_n) <_\tau (b_1, \dots, b_n) \text{ iff } n = m + 1$$

and $a_i = b_i$ for $i = 1 \cdots m$.

Define the *length* $|T|$ of T to be $|(a_\tau)|_{<_\tau}$.

1.4.4. DEFINITION. If Φ is a rule set, a tree T is a Φ -proof of a if $a = a_T$ and $\Phi : T_{(a_1, \dots, a_n)} \rightarrow a_n$ whenever $(a_1, \dots, a_n) \in T$, where

$$T_{(a_1, \dots, a_n)} = \{a \mid (a_1, \dots, a_n, a) \in T\}.$$

1.4.5. PROPOSITION. (i) $I(\Phi) = \{a \mid a \text{ has a tree } \Phi\text{-proof}\}$.

(ii) If Φ is a rule set on A with corresponding monotone operator $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$, then for all ordinals λ ,

$$\varphi^\lambda = \{a \in A \mid a \text{ has a tree } \Phi\text{-proof of length } \leq \lambda\}.$$

PROOF. (i) follows easily from (ii). (ii) will be proved by induction on λ . Let X^λ denote the right-hand side of (ii) and let $X^{<\lambda} = \bigcup_{\mu < \lambda} X^\mu$. By induction hypothesis $\varphi^{<\lambda} = X^{<\lambda}$.

Let $a \in X^\lambda$. Then a has a Φ -proof T with $|T| \leq \lambda$. For each $x \in T_{(a)}$ let

$$T^x = \{(x, x_1, \dots, x_n) \mid n \geq 0 \ \& \ (a, x, x_1, \dots, x_n) \in T\}.$$

Then T^x is a Φ -proof of x with $|T^x| < \lambda$. Hence $T_{(a)} \subseteq X^{<\lambda} = \varphi^{<\lambda}$. As $\Phi : T_{(a)} \rightarrow a$ it follows that $a \in \varphi(\varphi^{<\lambda}) = \varphi^\lambda$.

Conversely, let $a \in \varphi^\lambda$. Then $a \in \varphi(X^{<\lambda})$. For each $x \in X^{<\lambda}$ let T^x be a Φ -proof of x with $|T^x| < \lambda$. Let

$$T = \{(a)\} \cup \{(a, x, x_1, \dots, x_n) \mid n \geq 0 \ \& \ x \in X^{<\lambda} \ \& \ (x, x_1, \dots, x_n) \in T^x\}.$$

Then T is a Φ -proof of a with $|T| \leq \lambda$, so that $a \in X^\lambda$. $\square$

1.5. Monotone induction and games

For those familiar with the elementary concepts associated with games we give a game-theoretic characterization of $I(\Phi)$ for an arbitrary rule set Φ .

For each a we define a game $G(\Phi, a)$ between two players I and II who move alternatively when possible. The play starts by II choosing $a_0 = a$. If after n pairs of moves player II chooses a_n then player I must respond by choosing a set X_n such that $\Phi : X_n \rightarrow a_n$ and then II must respond by choosing $a_{n+1} \in X_n$. If either player cannot move then he loses. If the game continues indefinitely, then player I loses.

1.5.1. PROPOSITION. $a \in I(\Phi)$ iff player I has a winning strategy in the game $G(\Phi, a)$.

PROOF. Let W be the set of those a such that the right-hand side holds. Let $\Phi : X \rightarrow a$ with $X \subseteq W$. For each $x \in X$ let σ_x be a winning strategy for I in $G(\Phi, x)$. Define the following strategy σ for I in $G(\Phi, a)$. I starts by

playing X and then if II chooses $x \in X$ then I continues by using the strategy σ_x . σ is clearly a winning strategy. Hence $a \in W$. Thus W is Φ -closed so that by Φ -induction $I(\Phi) \subseteq W$.

For the converse let $a \in W$. Let σ be a winning strategy for I in $G(\Phi, a)$. Let T be the set of possible finite sequences of moves of II when I follows σ . Then observe that T is a tree Φ -proof of a so that by Proposition 1.4.5, $a \in I(\Phi)$. Thus $W \subseteq I(\Phi)$. $\square$

1.6. Kernels — the dual of an inductive definition

Sometimes inductive definitions present themselves more naturally in a dual form.

If Φ is a rule set let us say that a set X is Φ -dense if for every $x \in X$ there is a set $Y \subseteq X$ such that $\Phi : Y \rightarrow x$. Define the *kernel* $K(\Phi) = \bigcup \{X \mid X \text{ is } \Phi\text{-dense}\}$. $K(\Phi)$ itself is Φ -dense and is the largest Φ -dense set. If Φ is a rule set on A and $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$ is the monotone operator associated with Φ then $X \subseteq A$ is Φ -dense iff $X \subseteq \varphi(X)$. Hence $K(\Phi) = \bigcup \{X \subseteq A \mid X \subseteq \varphi(X)\}$ and we shall define $K(\varphi) = \bigcup \{X \subseteq A \mid X \subseteq \varphi(X)\}$ for any monotone φ . To make explicit the duality between the kernel construction and induction define the *dual* of an operator φ to be the operator $\check{\varphi}$ given by $\check{\varphi}(X) = \neg \varphi(\neg X)$ where $\neg X = A - X$ for $X \subseteq A$. Then $X \subseteq A$ is φ -dense iff $\neg X$ is φ -closed, so that $K(\varphi) = \neg I(\check{\varphi})$. It follows that $K(\varphi)$ can be defined in terms of transfinite iterations $\varphi^{[\lambda]} = \neg \check{\varphi}^\lambda$, as $K(\varphi) = \bigcap_\lambda \varphi^{[\lambda]}$ where $\varphi^{[\lambda]} = \varphi(\bigcap_{\mu < \lambda} \varphi^{[\mu]})$.

An example of the above is the Cantor-Bendixson construction in general topology. Let E be a subset of a topological space. Let Φ be the set of rules $X \rightarrow x$ such that $X \subseteq E$ and $x \in E$ is a limit point of X . The corresponding monotone operator $\varphi : \text{Pow}(E) \rightarrow \text{Pow}(E)$ is the closure operation on E . A set $X \subseteq E$ is closed in E just in case X is Φ -closed and is dense in itself just in case it is Φ -dense. Thus $K(\varphi)$ is the largest dense in itself subset of E , called the kernel K of E . When E is a closed subset of a space with a countable basis then $E = K \cup S$ where K is perfect and $S = \neg K = I(\check{\varphi})$ is a countable set, so that the closure ordinal $|\check{\varphi}|$ must be countable. This is the Cantor-Bendixson representation of a closed subset of a space with a countable basis.

Another example of the kernel construction comes from the theory of abelian p -groups. These are abelian groups where every element has finite order p^n for some n , where p is a fixed prime. Let G be an abelian p -group. Define $\varphi : \text{Pow}(G) \rightarrow \text{Pow}(G)$ by

$$\varphi(X) = pX = \overbrace{\{g + \cdots + g \mid g \in X\}}^p \quad \text{for } X \subseteq G.$$

Then φ is a monotone operator mapping subgroups of G to subgroups of G . The φ -dense subgroups of G are just those that are said to be divisible, so that $K(\varphi)$ is the largest divisible subgroup of G . Much of the structure theory of abelian p -groups is concerned with the descending hierarchy of subgroups $\{\varphi^{[\lambda]}\}_\lambda$.

1.7. Some examples of induction in classical mathematics

(1) If X is a subset of a group G then there is a smallest subgroup H of G that contains X . H is inductively defined by the set of rules $\emptyset \rightarrow x$ for $x \in X \cup \{e\}$ and $\{a, b\} \rightarrow ab^{-1}$ for $a, b \in G$. The same notion is used with other algebraic structures such as rings, fields and vector spaces. A slightly different sort of example is the algebraic closure of a subfield of an algebraically closed field. All these examples involve finitary rule sets.

(2) If R is a binary relation on a set A , then the transitive closure of R is the smallest transitive relation extending R . It is inductively defined by the set of rules $\emptyset \rightarrow (a, b)$ if aRb and $\{(a, b), (b, c)\} \rightarrow (a, c)$ for $a, b, c \in A$. Similarly the equivalence relation generated by R is inductively defined by the above rules together with the rules $\emptyset \rightarrow (a, a)$ for $a \in A$ and $\{(a, b)\} \rightarrow (b, a)$ for $a, b \in A$.

(3) For an example of a non-finitary inductive definition we turn to σ -rings and Borel sets. Recall that a set $\mathcal{C} \subseteq \text{Pow}(A)$ is σ -ring if it is closed under complements and unions of countable subsets; i.e., combining these into one $\mathcal{C}$ is a σ -ring if $\mathcal{C}$ is Φ -closed where Φ consists of the rules $\{A_n \mid n \in \omega\} \rightarrow \bigcup_{n < \omega} \neg A_n$ for countable families $\{A_n\}_{n \in \omega}$ with $A_n \subseteq A$. Hence the σ -ring generated by $\mathcal{C}_0 \subseteq \text{Pow}(A)$ is inductively defined by the rule set Φ' consisting of the rules in Φ together with the rules $\emptyset \rightarrow X$ for $X \in \mathcal{C}_0$. As an example the Borel sets of reals are the special case where $A = \mathbb{R}$ and $\mathcal{C}_0$ is the set of open subsets of $\mathbb{R}$. If $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$ is the monotone operator associated with Φ' then φ is $\aleph_1$ -based so that by Proposition 1.3.4, $|\varphi| \leq \aleph_1$. The stages φ^λ for $\lambda < \aleph_1$ are just the familiar stages of the Borel hierarchy. φ^0 is the set of open sets and for $\lambda > 0$, the sets in φ^λ are those of the form $\bigcup_{n < \omega} \neg A_n$ where each $A_n \in \varphi^{<\lambda}$.

2. Induction in recursion theory

2.1. Recursively enumerable relations

There are two key results relating the recursively enumerable (r.e.) relations to the finitely presented formal systems such as formal arithmetic:

(I) The theorems of a finitely presented formal system form an r.e. set, when Gödel numbered.

(II) Every r.e. relation can be represented in any sufficiently rich formal system.

These results are important in Gödel's incompleteness theorem. The general notion of representability will be considered in the next section. Here we wish to give a result concerning inductive definitions that yields I.

As we have seen, a formal system will determine a rule set that inductively defines the set of theorems. When expressions are Gödel numbered, a rule set on ω is induced that inductively defines the set of Gödel numbers of theorems. If the formal system is finitely presented the rule set will be a recursive finitary one as defined below.

2.1.1. DEFINITION. Let Φ be a finitary rule set on ω . Φ is *recursive* (r.e.) if the relation R_Φ is recursive (r.e.) where R_Φ is the set of pairs $\langle \langle a_1, \dots, a_n \rangle, b \rangle$ such that $\Phi : \{a_1, \dots, a_n\} \rightarrow b$.

Here $\langle \rangle : \bigcup_{n \in \omega} \omega^n \rightarrow \omega$ is a standard constructive injective coding function for finite sequences of natural numbers. Associated with it are recursive functions $\text{lh} : \omega \rightarrow \omega$ and $q : \omega \times \omega \rightarrow \omega$ and they satisfy the following:

- (i) The range Seq of $\langle \rangle$ is recursive.
- (ii) For each $n > 0$ the function $\langle \rangle \upharpoonright \omega^n : \omega^n \rightarrow \omega$ is recursive.
- (iii) $\text{lh}(\langle x_1, \dots, x_n \rangle) = n$ for $n \geq 0$.
- (iv) $q(\langle x_1, \dots, x_n \rangle, i) = x_i$ for $1 \leq i \leq n$.

2.1.2. PROPOSITION. If Φ is an r.e. finitary rule set on ω , then $I(\Phi)$ is r.e.

PROOF. As Φ is finitary, by Proposition 1.1.4,

$$I(\Phi) = \{a \in \omega \mid \exists y \text{Pr}_\Phi(a, y)\}$$

where $\text{Pr}_\Phi(a, b)$ iff $b = \langle a_1, \dots, a_n \rangle$ for some Φ -proof $a_1, \dots, a_n$ of b . Hence to prove the proposition it suffices to show that Pr_Φ is r.e. But this is just a matter of coding:

$$\begin{aligned} \text{Pr}_\Phi(a, b) &\Leftrightarrow \text{Seq}(b) \ \& \ q(b, \text{lh}(b)) = a \\ &\ \& \ \forall i < \text{lh}(b) \exists z [\text{R}_\Phi(z, q(b, i+1)) \\ &\ \& \ \forall i < \text{lh}(z)) \exists k < i (q(z, i+1) = q(x, k+1))]. \end{aligned}$$

By hypothesis, using standard closure properties of the r.e. relations we see that the right-hand side is r.e. $\square$

2.2. Π_1^1 relations

When infinitary rules of inference are allowed in a formal system then more general notions of induction are required, e.g. in GRZEGORCZYK, MOSTOWSKI and RYLL-NARDZEWSKI [1958] the ω -rule is added to an otherwise finitely presented formal system for second order arithmetic. The ω -rule allows one to infer $\forall x \varphi(x)$ from an infinite set of premisses $\varphi(0), \varphi(1), \dots$. When Gödel numbered, such a formal system induces a regular arithmetical rule set Φ on ω .

2.2.1. DEFINITION. A rule set Φ on ω is *regular arithmetical* if there are arithmetical relations R and S such that Φ is the set of rules $R_a \rightarrow b$ such that $S(a, b)$ where $R_a = \{y \in \omega \mid R(a, y)\}$.

2.2.2. PROPOSITION. (i) If Φ is a regular arithmetical rule set on ω , then the associated monotone operator $\varphi : \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ is Π_1^1 (i.e., $\{(X, x) \in \text{Pow}(\omega) \times \omega \mid x \in \varphi(X)\}$ is Π_1^1).

(ii) For any monotone $\Pi_1^1 \varphi$ the set $I(\varphi)$ is also Π_1^1 .

PROOF. (i) Let Φ be the set of rules $R_a \rightarrow b$ such that $S(a, b)$ where R, S are arithmetical. Then the associated monotone operator φ is given by $\varphi(X) = \{b \in \omega \mid \exists a [S(a, b) \ \& \ R_a \subseteq X]\}$ for $X \subseteq A$. φ is arithmetical and hence Π_1^1 .

(ii) $I(\varphi) = \{a \in \omega \mid \forall X [\forall x [x \in \varphi(X) \rightarrow x \in X] \rightarrow a \in X]\}$ so that if φ is Π_1^1 standard quantifier manipulations show that $I(\varphi)$ is also Π_1^1 . $\square$

Hence when considering systems with the ω -rule the above proposition suggests that the class of r.e. relations in I and II of 2.1. should be replaced by the class of Π_1^1 relations.

Below we give two further examples of regular arithmetical rule sets.

The first example occurs in the definition of Kleene's system of notations for the recursive ordinals. This may be given as follows. Let $<$ be the smallest transitive relation on ω such that

(i) $a < 2^a$ for $a \in \omega$,

(ii) $\{e\}(n) < 3 \cdot 5^e$ for $e, n \in \omega$ such that $\{e\}(n)$ is defined. (Here $\{e\}$ is the e -th partial recursive function in a standard enumeration.) Then $<$ is easily seen to be an r.e. relation. Now let Φ be the set of rules $\emptyset \rightarrow 1$, $\{a\} \rightarrow 2^a$ for $a \in \omega$, and $\{\{e\}(n) \mid n < \omega\} \rightarrow 3 \cdot 5^e$ for $e \in \omega$ such that $\{e\}(n)$ is defined and $\{e\}(n) < \{e\}(n+1)$ for all $n \in \omega$. Then let $\mathcal{O} = I(\Phi)$. Let $a <_0 b$ iff $a, b \in \mathcal{O}$ & $a < b$. As Φ is regular arithmetical, $\mathcal{O}$ and hence $<_0$ are Π_1^1 . For $a \in \mathcal{O}$ let $|a|_0 = |a|_\varphi$. Then $|1|_0 = 0$, $|2^a|_0 = |a|_0 + 1$ for $a \in \mathcal{O}$ and $|3 \cdot 5^e|_0 = \lim_{n \in \omega} |\{e\}(n)|_0$ for $3 \cdot 5^e \in \mathcal{O}$. Thus $(\mathcal{O}, <_0, | \cdot |_0)$ is Kleene's recur-

sive analogue of the countable ordinals. The ordinal $|\varphi| = \text{Sup}\{|a|_0 + 1 \mid a \in \mathcal{O}\}$ is the Church-Kleene ordinal ω_1 , the first admissible ordinal $> \omega$.

As another example of a regular arithmetical induction we consider the hyperarithmetical hierarchy as formulated in MOSCHOVAKIS [1974a]. This is a recursive analogue of the Borel hierarchy. Call a set $\mathcal{B} \subseteq \text{Pow}(\omega)$ an *effective σ -ring* if $\mathcal{B}$ effectively contains the r.e. sets and is effectively closed under complementation and countable unions. I.e., there is a set $I \subseteq \omega$ and sets $B_i \subseteq \omega$ for $i \in I$ such that $\mathcal{B} = \{B_i \mid i \in I\}$ and:

- (i) There is a recursive function $\tau_1: \omega \rightarrow I$ such that $R_e = B_{\tau_1(e)}$ for all $e \in \omega$. (Recall that R_e is the e -th r.e. set in a standard enumeration.)
- (ii) There is a recursive function $\tau_2: \omega \rightarrow \omega$ such that if $\{e\}$ is a total function $f: \omega \rightarrow I$, then

$$\tau_2(e) \in I \quad \text{and} \quad B_{\tau_2(e)} = \bigcup_{n < \omega} \neg B_{f(n)}.$$

An effective σ -ring may be constructed as follows. Let $\tau_1(n) = 2^n$. Let $\tau_2(e) = 3 \cdot 5^e$. Let Φ be the set of rules $\emptyset \rightarrow \tau_1(n)$ for $n \in \omega$ and $\{f(n) \mid n \in \omega\} \rightarrow \tau_2(e)$ for $e \in \omega$ such that $\{e\}$ is a totally defined function f . Let $I = I(\Phi)$. Then Φ is a deterministic rule set (see 1.2) so that by recursion we may define $B_e \subseteq \omega$ for $e \in I$ by

$$B_{\tau_1(e)} = R_e \quad \text{for } e \in \omega,$$

$$B_{\tau_2(e)} = \bigcup_{n \in \omega} \neg B_{f(n)} \quad \text{if } \{e\} = f: \omega \rightarrow I.$$

Then clearly $\mathcal{B} = \{B_i \mid i \in I\}$ is an effective σ -ring.

As Φ is regular arithmetical, $I = I(\Phi)$ is Π_1^1 . Let φ be the monotone operator associated with Φ . $\mathcal{B}$ can be arranged in a hierarchy $\mathcal{B} = \bigcup_{\lambda < \omega_1} \mathcal{B}^\lambda$ where $\mathcal{B}^\lambda = \{B_e \mid e \in \varphi^\lambda\}$ for $\lambda < \omega_1$ ($= |\varphi|$). So $\mathcal{B}^0$ is the set of r.e. sets, $\mathcal{B}^1$ is the set of Σ_2^0 sets, $\bigcup_{n < \omega} \mathcal{B}^n$ is the set of arithmetical sets. In Section 8E of MOSCHOVAKIS [1974a] there is a proof of the following result.

2.2.3. THEOREM. *$\mathcal{B}$ is the smallest effective σ -ring and coincides with the set of Δ_1^1 subsets of ω .*

2.3. Representability

In this subsection we generalize the approach to the recursively enumerable and Π_1^1 relations on ω in terms of representability to arbitrary structures.

Suppose that we have a set A and a theory T that has individual

constants for elements of A as well as individual variables. (The same symbol will be used for a constant and the object it names.)

2.3.1. DEFINITION. $R \subseteq A^n$ is T -represented by the formula $\theta(\bar{x})$ if $\bar{x} = x_1, \dots, x_n$ and

$$R(\bar{a}) \Leftrightarrow T \vdash \theta(\bar{a}) \quad \text{for } \bar{a} \in A^n.$$

If $A = \omega$ and T is a finitely presented theory such as formal arithmetic, then the set $^{\ulcorner}T^{\urcorner}$ of Gödel numbers $^{\ulcorner}\theta^{\urcorner}$ of theorems θ of T forms an r.e. set and hence every T -representable relation is also r.e. For if R is T -represented by $\theta(\bar{x})$, then $R(\bar{a}) \Leftrightarrow f(\bar{a}) \in ^{\ulcorner}T^{\urcorner}$ for $\bar{a} \in \omega^n$, where f is the recursive function given by $f(\bar{a}) = ^{\ulcorner}\theta(\bar{a})^{\urcorner}$ for $\bar{a} \in \omega^n$. Result II of 2.1 gives a converse of this result for sufficiently rich T . Hence for suitable systems T , the T -representable relations are exactly the r.e. relations.

Ordinary recursion theory can be developed from scratch by making a suitable choice of T . For example Post's canonical systems (see POST [1943]) make one such choice, which is further refined in SMULLYAN [1961]. Kleene's systems of equations for representing the partial recursive functions (see KLEENE [1952]) give another approach.

In GRZEGORCZYK, MOSTOWSKI and RYLL-NARDZEWSKI [1958] it is shown that in second order formal arithmetic with the ω -rule exactly the Π_1^1 relations are representable. Hence the notion of representability gives a way of uniformly treating the r.e. relations and the Π_1^1 relations. Below we give such a uniform treatment for arbitrary structures $\mathfrak{A}$ that gives these classes of relations on ω when $\mathfrak{A}$ is the structure $\mathfrak{N} = \langle \omega, S, P \rangle$ of arithmetic where S and P are the graphs of addition and multiplication.

First we need to give some definitions. Given a set A we introduce the full first order language L^A over A . L^A has individual constants for the elements of A and related constants for the relations on A . There are also individual variables and n -ary relation variables for each $n > 0$.

The *elementary* (i.e. first order) formulae of L^A are built up in the usual way using the connectives and the individual quantifiers $\forall x, \exists x$. The second order formulae are obtained by allowing quantifiers $\forall X^n, \exists X^n$ where X^n is an n -place relation variable. All elementary or second order sentences of L^A are either true or false in the standard interpretation. We shall be interested in various subclasses of formulae. The *existential* formulae are built up from atomic formulae and their negations using $\vee, \wedge$ and $\exists x$. Given a binary relation $<$ on A we may introduce the restricted quantifiers $\forall x < y, \exists x < y$ abbreviating $\forall x (x < y \rightarrow$ and $\exists x (x < y \wedge$. Then we may define the restricted elementary formulae as those built up

using only restricted quantifiers. We may define the Σ_n^0 and Π_n^0 prenex formulae, where we allow the matrix to be restricted, in the usual way, e.g. Σ_2^0 formulae have the form $\exists x_1 \cdots \exists x_n \forall y_1 \cdots \forall y_m \theta$, where $n, m \geq 0$ and θ is restricted.

We will also be interested in classifications of second order formulae. A formula is Π_1^1 if it has the form $\forall X_1 \cdots \forall X_m \theta$ where $m \geq 0$ and θ is elementary. Similarly we define the Π_n^1 and Σ_n^1 formulae for $n > 0$, by counting the number of alternating blocks of relation quantifiers.

Given a structure $\mathfrak{A} = \langle A, R_1, \dots, R_l \rangle$ $L(\mathfrak{A})$ is the sublanguage of L^A that only allows relation constants for equality and the relations $R_1, \dots, R_l$. If $\mathcal{F}$ is a collection of formulae of L^A , then $R \subseteq A^n$ is $\mathcal{F}$ -definable over $\mathfrak{A}$ if there is a formula $\theta(\bar{x})$ of $L(\mathfrak{A})$ in $\mathcal{F}$ such that $\bar{x} = x_1, \dots, x_n$ includes all the free variables of $\theta(\bar{x})$ and

$$R(\bar{a}) \Leftrightarrow \theta(\bar{a}) \text{ is true for } \bar{a} \in A^n.$$

Many constructions in ordinary recursion theory make use of some coding apparatus, e.g. in Gödel numbering. To extend such constructions to $\mathfrak{A}$ we shall need such apparatus to be definable on $\mathfrak{A}$ in a suitable way.

2.3.2. DEFINITION. A *coding scheme* for A is a triple $\mathcal{C} = \langle N, \leq, \langle \rangle \rangle$ where:

(i) $N \subseteq A$ and $\leq$ is a binary relation on N such that $\langle N, \leq \rangle \cong \langle \omega, \leq \rangle$. We shall identify N with $\omega = \{0, 1, \dots\}$.

(ii) $\langle \rangle: \bigcup_{n \in \omega} A^n \rightarrow A$ is an injective function. Associated with $\mathcal{C}$ are the following.

(iii) Seq, the set of codes of finite sequences is the range of $\langle \rangle$.

(iv) $lh: \text{Seq} \rightarrow N$ is given by $lh(\langle x_1, \dots, x_n \rangle) = n$.

(v) $q: \text{Seq} \times N \rightarrow A$ is given by

$$q(\langle x_1, \dots, x_n \rangle, i) = \begin{cases} x_i & \text{if } 1 \leq i \leq n, \\ 0 & \text{otherwise.} \end{cases}$$

(vi) $s: N \rightarrow N$ is given by $s(n) = n + 1$.

If $\mathcal{F}$ is a class of formulae we say that $\mathcal{C}$ is $\mathcal{F}$ -definable over $\mathfrak{A}$ if $N, \leq, \text{Seq}$ and the graphs of lh, q and s are $\mathcal{F}$ -definable over $\mathfrak{A}$.

$\mathfrak{A}$ is $\mathcal{F}$ -acceptable if there is a coding scheme $\mathcal{C}$ over A that is $\mathcal{F}$ -definable over $\mathfrak{A}$. In case $\mathcal{F}$ is the class of elementary formulae we just write *acceptable* for $\mathcal{F}$ -acceptable.

Given a coding scheme $\mathcal{C}$ over A and a structure $\mathfrak{A}$, formulae θ of $L(\mathfrak{A})$ can be assigned "Gödel numbers" $\ulcorner \theta \urcorner \in A$ in a standard way. We shall not

go into the details of this here but shall occasionally need to make use of certain facts about such a Gödel numbering.

Given a structure $\mathfrak{A}$ let $T(\mathfrak{A})$ be the formal system, in the first order language $L(\mathfrak{A})$, that has a standard system of axioms and rules of inference for first order logic with equality and has the diagram of $\mathfrak{A}$ as a set of non-logical axioms. So every true sentence of $L(\mathfrak{A})$, that is atomic or the negation of an atomic sentence, is an axiom of $T(\mathfrak{A})$.

Our generalization of the class of r.e. relations on ω is the class of $T(\mathfrak{A})$ -representable relations on A . For this to be a good notion we shall require that $\mathfrak{A}$ is existentially acceptable with an existentially definable coding scheme $\mathcal{C}$. Let $<$ be the relation on A that is the strict ordering relation of the copy of the natural numbers on A given by $\mathcal{C}$. Let $\Sigma_1^0(\mathfrak{A})$ be the class of relations on A that are Σ_1^0 definable over $\mathfrak{A}$, where the above $<$ relation is used in defining restricted formulae. As on ω , we can show that the finitary rule set inductively defining the theorems of A , induces a $\Sigma_1^0(\mathfrak{A})$ finitary rule set on A .

2.3.3. DEFINITION. A finitary rule set Φ on A is $\Sigma_1^0(\mathfrak{A})$ if the relation R_Φ is $\Sigma_1^0(\mathfrak{A})$ where R_Φ is the set of pairs $\langle \langle a_1, \dots, a_n \rangle, b \rangle$ such that $\Phi : \{a_1, \dots, a_n\} \rightarrow b$.

The following is proved exactly as Proposition 2.2.2.

2.3.4. PROPOSITION. If $\mathfrak{A}$ is existentially acceptable and Φ is a $\Sigma_1^0(\mathfrak{A})$ finitary rule set, then $I(\Phi)$ is also $\Sigma_1^0(\mathfrak{A})$.

2.3.5. COROLLARY. If $\mathfrak{A}$ is existentially acceptable, then $\lceil T(\mathfrak{A}) \rceil$ is $\Sigma_1^0(\mathfrak{A})$ and hence every $T(\mathfrak{A})$ -representable relation is $\Sigma_1^0(\mathfrak{A})$.

To prove the last part we need the fact that if $\theta(\bar{x})$ is a formula and $f(\bar{a}) = \lceil \theta(\bar{a}) \rceil$ for $\bar{a} \in A^n$, then the graph of f is in $\Sigma_1^0(\mathfrak{A})$. The converse to this will be given in the next section.

Let us now generalize the ω -rule. The system $T_\infty(\mathfrak{A})$ is obtained from $T(\mathfrak{A})$ by adding the following infinitary rule

A-rule: From $\theta(a)$ for $a \in A$ infer $\forall x \theta(x)$.

Let us call an elementary formula $\varphi(X_1, \dots, X_m, x_1 \cdots x_n)$ of $L(\mathfrak{A})$ *universally true* if the Π_1^0 sentence

$$\forall X_1 \cdots \forall X_m \forall x_1 \cdots \forall x_n \varphi(X_1, \dots, X_m, x_1, \dots, x_n)$$

is true. It is easily seen that the axioms of $T_\infty(\mathfrak{A})$ are all universally true and all the rules of inference of $T_\infty(\mathfrak{A})$ preserve universal truth. Hence we have:

2.3.6. PROPOSITION. $T_\infty(\mathfrak{A}) \vdash \varphi$ implies φ is universally true.

In case $\mathfrak{A}$ is countable a completeness theorem holds that gives the converse to Proposition 2.3.6. It can be proved using the omitting types theorem for countable first order languages (see CHANG and KEISLER [1973]) or else it can be proved by a direct Henkin construction, as in GRILLIOT [1974].

2.3.7. THEOREM. For countable $\mathfrak{A}$,

$$T_\infty(\mathfrak{A}) \vdash \varphi \quad \text{iff} \quad \varphi \text{ is universally valid.}$$

2.3.8. COROLLARY. For countable $\mathfrak{A}$ a relation on A is $T_\infty(\mathfrak{A})$ -representable iff it is $\Pi_1^1(\mathfrak{A})$ (i.e. Π_1^1 -definable over $\mathfrak{A}$).

PROOF. By Theorem 2.3.7, $\theta(\bar{x})$ $T_\infty(\mathfrak{A})$ -represents R iff $\forall X_1 \cdots \forall X_m \theta(\bar{x})$ defines R , where $X_1, \dots, X_m$ are the relation variables occurring in the elementary formula $\theta(\bar{x})$. This result includes the special case of arithmetic when $\mathfrak{A} = \mathfrak{N}$. $\square$

As before, if we assume given a coding scheme $\mathcal{C}$ over $\mathfrak{A}$, the rule set inductively defining the theorems of $T_\infty(\mathfrak{A})$ when Gödel numbered induces a rule set on A that has the following property when $\mathcal{C}$ is elementary over $\mathfrak{A}$.

2.3.9. DEFINITION. A rule set Φ on A is *regular elementary over* $\mathfrak{A}$ if there are elementary relations R, S such that Φ is the set of rules $R_a \rightarrow b$ such that $S(a, b)$.

2.3.10. PROPOSITION. If $\mathfrak{A}$ is an acceptable structure, then there is a regular elementary rule set Φ such that $\lceil T_\infty(\mathfrak{A}) \rceil = I(\Phi)$.

This result will be needed in the next section.

Finally we consider the notion of truth for (elementary) sentences of $L(\mathfrak{A})$. It is easily seen that every true sentence can be proved in $T_\infty(\mathfrak{A})$ and hence we have the characterization. If φ is a sentence of $L(\mathfrak{A})$ φ is true iff

$T_{\infty}(\mathfrak{A}) \vdash \varphi$. Alternatively we may give the usual inductive definition for truth that follows the way φ is built up. This can be expressed as follows. Let us call expressions of the form $+\varphi$ or $-\varphi$ where φ is a sentence of $L(\mathfrak{A})$, *labelled* sentences. Now let Φ be the following set of rules on labelled sentences.

$\emptyset \rightarrow +\theta$ for each true atomic sentence θ ,

$\emptyset \rightarrow -\theta$ for each false atomic sentence θ ;

$\{+\varphi, +\psi\} \rightarrow +(\varphi \wedge \psi)$ for sentences φ, ψ ,

$\{-\varphi\} \rightarrow -(\varphi \wedge \psi)$ for sentences φ, ψ ,

$\{-\psi\} \rightarrow -(\varphi \wedge \psi)$ for sentences φ, ψ ;

similar rules for $\neg, \vee, \rightarrow$;

$\{+\varphi(a) \mid a \in A\} \rightarrow +\forall x \varphi(x)$ for sentence $\forall x \varphi(x)$,

$\{-\varphi(a)\} \rightarrow -\forall x \varphi(x)$ for $a \in A$;

and similar rules for $\exists x$.

Then if φ is a sentence,

φ is true iff $+\varphi \in I(\Phi)$,

φ is false iff $-\varphi \in I(\Phi)$.

Note again, that when Gödel numbered, using an elementary coding scheme, the above rule set Φ induces a regular elementary rule set on A .

3. Classes of inductive definitions

3.1. The general framework

Much recent work on inductive definitions falls under the following general framework. Assume given an infinite set A . Let $\mathcal{E}$ be a class of operators, each of the form $\varphi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ for some $n > 0$.

3.1.1. DEFINITION. (i) $R \subseteq A^n$ is $\mathcal{E}$ -inductive if there is $\varphi : \text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$ in $\mathcal{E}$ with $m \geq n$ and $\bar{b} \in A^{m-n}$ such that for $\bar{a} \in A^n$,

$$R(\bar{a}) \Leftrightarrow (\bar{b}, \bar{a}) \in \varphi^{\infty}.$$

(ii) $\text{IND}(\mathcal{E})$ is the set of $\mathcal{E}$ -inductive relations.

(iii) $|\mathcal{E}| = \text{Sup}\{|\varphi| \mid \varphi \in \mathcal{E}\}$.

Why not define $\text{IND}(\mathcal{E})$ to be $\{\varphi^\infty \mid \varphi \in \mathcal{E}\}$? This turns out not to be natural, as we will want $\text{IND}(\mathcal{E})$ to have certain closure properties, e.g. we generally want $\text{IND}(\mathcal{E})$ to be closed under intersections and there seem to be no reasonable conditions on $\mathcal{E}$ that will ensure this for $\{\varphi^\infty \mid \varphi \in \mathcal{E}\}$. We give a general result below that gives closure properties of $\text{IND}(\mathcal{E})$ given suitable assumptions on $\mathcal{E}$.

Call $\tau : A^n \rightarrow A^m$ a *section map* if $m \geq n$ and for some $\bar{b} \in A^{m-n}$,

$$\tau(\bar{a}) = (\bar{b}, \bar{a}) \quad \text{for all } \bar{a} \in A^n.$$

Then $\text{IND}(\mathcal{E}) = \{\tau^{-1}\varphi^\infty \mid \varphi \in \mathcal{E} \text{ \& } \tau \text{ is a section map}\}$.

Section maps are used to code several inductive definitions into one. The following is the key to this.

3.1.2. LEMMA. *Let $n_1, \dots, n_k > 0$ and $m \geq \max(n_1, \dots, n_k) + 1$. Then there are section maps $\tau_1 : A^{n_1} \rightarrow A^m, \dots, \tau_k : A^{n_k} \rightarrow A^m$ that have pairwise disjoint ranges.*

PROOF. Choose pairwise distinct elements $c_1, \dots, c_k \in A$ and define

$$\tau_i(\bar{a}) = (\overbrace{c_i, \dots, c_i}^{m-n_i}, \bar{a}) \in A^m \quad \text{for } \bar{a} \in A^{n_i}. \quad \square$$

3.1.3. DEFINITION. An operator

$$\theta : \text{Pow}(A^{n_1}) \times \dots \times \text{Pow}(A^{n_k}) \rightarrow \text{Pow}(A^n)$$

is *section codable* in $\mathcal{E}$ if for section maps $\tau_1 : A^{n_1} \rightarrow A^m, \dots, \tau_k : A^{n_k} \rightarrow A^m$, $\tau : A^n \rightarrow A^m$ $\varphi \in \mathcal{E}$ where $\varphi : \text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$ is given by

$$\varphi(S) = \tau\theta(\tau_1^{-1}S, \dots, \tau_k^{-1}S) \quad \text{for } S \subseteq A^m.$$

3.1.4. PROPOSITION. *If (i) $\mathcal{E}$ is closed under unions (i.e. $\varphi, \psi \in \mathcal{E}$ implies $\varphi \cup \psi \in \mathcal{E}$, where $\varphi \cup \psi(S) = \varphi(S) \cup \psi(S)$),*

(ii) every operator in $\mathcal{E}$ is section codable in $\mathcal{E}$, then $\text{IND}(\mathcal{E})$ is closed under every operator $\theta : \text{Pow}(A^{n_1}) \times \dots \times \text{Pow}(A^{n_k}) \rightarrow \text{Pow}(A^n)$ that is section codable in $\mathcal{E}$ and is monotone in each argument.

PROOF. Let θ be as above, section codable in $\mathcal{E}$ and monotone in each argument. Let $R_i = \sigma_i^{-1}\varphi_i^\infty$ where $\sigma_i : A^{n_i} \rightarrow A^{m_i}$ is a section map and $\varphi_i : \text{Pow}(A^{m_i}) \rightarrow \text{Pow}(A^{m_i})$ is in $\mathcal{E}$ for $i = 1, \dots, k$. We wish to show that $\theta(R_1, \dots, R_k) = \tau^{-1}\varphi^\infty$ for some section map τ and some $\varphi \in \mathcal{E}$.

Let $m = \max(m_1, \dots, m_k, n) + 1$, and choose section maps $\tau_1: A^{m_1} \rightarrow A^m, \dots, \tau_k: A^{m_k} \rightarrow A^m, \tau: A^n \rightarrow A^m$ with pairwise disjoint ranges. Let $\varphi'_i(S) = \tau_i \varphi_i(\tau_i^{-1} S)$ for $i = 1, \dots, k$ and $S \subseteq A^m$. Let $\theta'(S) = \tau \theta((\tau_1 \sigma_1)^{-1} S, \dots, (\tau_k \sigma_k)^{-1} S)$ for $S \subseteq A^m$. Finally let $\varphi(S) = \varphi'_1(S) \cup \dots \cup \varphi'_k(S) \cup \theta'(S)$ for $S \subseteq A^m$. By assumption (ii) each $\varphi'_i \in \mathcal{E}$. As θ is section codable in $\mathcal{E}$, $\theta' \in \mathcal{E}$. Hence by assumption (i) $\varphi \in \mathcal{E}$.

Now it is easy to see that $\varphi_i^\infty = \tau_i^{-1} \varphi^\infty$ so that $R_i = (\tau_i \sigma_i)^{-1} \varphi^\infty$ for $i = 1, \dots, k$. Also, $\tau^{-1} \varphi^\infty = \theta((\tau_1 \sigma_1)^{-1} \varphi^{<\infty}, \dots, (\tau_k \sigma_k)^{-1} \varphi^{<\infty})$. Hence as θ is monotone,

$$\begin{aligned} \tau^{-1} \varphi^\infty &= \bigcup_{\lambda} \tau^{-1} \varphi^\lambda \\ &= \bigcup_{\lambda} \theta((\tau_1 \sigma_1)^{-1} \varphi^{<\lambda}, \dots, (\tau_k \sigma_k)^{-1} \varphi^{<\lambda}) \\ &= \theta((\tau_1 \sigma_1)^{-1} \varphi^\infty, \dots, (\tau_k \sigma_k)^{-1} \varphi^\infty) \\ &= \theta(R_1, \dots, R_k). \quad \square \end{aligned}$$

Note. Monotonicity of θ is essential in the above theorem. In general $\text{IND}(\mathcal{E})$ will not be closed under complementation.

3.1.5. EXAMPLE. The basic first order monotone operators are $\vee^n$, $\wedge^n$, $\exists^n$ and $\forall^n$ for $n > 0$.

$$\begin{aligned} \vee^n(R, S) &= R \cup S \quad \text{for } R, S \subseteq A^n, \\ \wedge^n(R, S) &= R \cap S \quad \text{for } R, S \subseteq A^n; \\ \exists^n(R) &= \{\bar{a} \in A^n \mid \exists x R(x, \bar{a})\} \quad \text{for } R \subseteq A^{n+1}, \\ \forall^n(R) &= \{\bar{a} \in A^n \mid \forall x R(x, \bar{a})\} \quad \text{for } R \subseteq A^{n+1}. \end{aligned}$$

Usually the class $\mathcal{E}$ of operators is specified by definability conditions.

Let $\varphi(X, \bar{x})$ be a formula of L^A having free at most the n -ary relation variable X and the individual variables $\bar{x} = x_1, \dots, x_n$. We say that $\varphi(X, \bar{x})$ *defines the operator* $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ if

$$\varphi(S) = \{\bar{a} \in A^n \mid \varphi(S, \bar{a}) \text{ is true}\} \quad \text{for } S \subseteq A^n.$$

Given a class $\mathcal{F}$ of formulae of L^A and a structure $\mathfrak{A} = \langle A, R_1, \dots, R_l \rangle$ let $\mathcal{F}(\mathfrak{A})$ denote the class of operators definable by a formula of $\mathcal{F}$ in $L(\mathfrak{A})$. Let $\text{mon-}\mathcal{F}(\mathfrak{A})$ denote the subclass of monotone operators in $\mathcal{F}(\mathfrak{A})$. Finally let $\text{pos-}\mathcal{F}(\mathfrak{A})$ denote the class of operators definable by a formula $\varphi(X, \bar{x})$ of $\mathcal{F}$ in $L(\mathfrak{A})$ in which X occurs only positively, i.e. $\varphi(X, \bar{x})$ is built up from

formulae not involving X and atomic formulae involving X using only the positive connectives $\vee$, $\wedge$ and the quantifiers. Operators in $\text{pos-}\mathcal{F}(\mathfrak{A})$ are automatically monotone. So we have

$$\text{pos-}\mathcal{F}(\mathfrak{A}) \subseteq \text{mon-}\mathcal{F}(\mathfrak{A}) \subseteq \mathcal{F}(\mathfrak{A})$$

and hence

$$\text{IND}(\text{pos-}\mathcal{F}(\mathfrak{A})) \subseteq \text{IND}(\text{mon-}\mathcal{F}(\mathfrak{A})) \subseteq \text{IND}(\mathcal{F}(\mathfrak{A}))$$

$$\text{and } |\text{pos-}\mathcal{F}(\mathfrak{A})| \leq |\text{mon-}\mathcal{F}(\mathfrak{A})| \leq |\mathcal{F}(\mathfrak{A})|.$$

3.2. Positive existential induction

In this subsection we look at perhaps the simplest example of the general framework, i.e. we consider the class of operators $\text{pos-}\mathcal{F}(\mathfrak{A})$, where $\mathcal{F}$ is the class of existential formulae. We shall write $\text{IND}(\exists - \mathfrak{A})$ and $|\exists - \mathfrak{A}|$ for $\text{IND}(\text{pos-}\mathcal{F}(\mathfrak{A}))$ and $|\text{pos-}\mathcal{F}(\mathfrak{A})|$, when $\mathcal{F}$ is this class. We will see that for existentially acceptable $\mathfrak{A}$ the class $\text{IND}(\exists - \mathfrak{A})$ coincides with the $T(\mathfrak{A})$ -representable relations and gives a good generalization of the r.e. relations on ω .

3.2.1. PROPOSITION. *If $\mathfrak{A}$ is infinite, then*

$$|\exists - \mathfrak{A}| = \omega.$$

PROOF. $|\exists - \mathfrak{A}| \geq \omega$, as $|\varphi_n| = n$ for each $n \in \omega$ where

$$\varphi_n(X) = \left\{ x \in A \mid \bigvee_{i < n} \left[\bigwedge_{j < i} X(a_j) \wedge x = a_i \right] \right\} \quad \text{for } X \subseteq A,$$

where $a_0, \dots, a_{n-1}$ are pairwise distinct elements of A . Clearly each φ_n is positive existential, $\varphi_n^i = \{a_j \mid j < i\}$ for $i \leq n$ and hence $I(\varphi) = \{a_j \mid j < n\}$.

To show that $|\exists - \mathfrak{A}| \leq \omega$, by Proposition 1.3.4 it suffices to show that each positive existential operator φ is ω -based. For this it suffices to show that, for each existential formula $\theta(X)$ positive in the relation variable X and containing no other free variables, $\theta(R)$ is true implies $\theta(S)$ is true for some finite $S \subseteq R$. This is easily proved by induction on the way such formulae $\theta(X)$ are built up.

The next result gives closure properties for $\text{IND}(\exists - \mathfrak{A})$.

3.2.2. PROPOSITION. (i) *If $\theta : \text{Pow}(A^n) \times \dots \times \text{Pow}(A^{n_k}) \rightarrow \text{Pow}(A^n)$ is positive existential over $\mathfrak{A}$ (or equivalently is section codable in the class of positive existential operators), then $\text{IND}(\exists - \mathfrak{A})$ is closed under θ . Hence the relations $=, R_1, \dots, R_i$ and their complements are $\text{IND}(\exists - \mathfrak{A})$, as the appropriate constant operators are positive existential over $\mathfrak{A}$. Also*

$\text{IND}(\exists - \mathfrak{A})$ is closed under $\vee^n$, $\wedge^n$, $\exists^n$ for $n > 0$ as these are positive existential over $\mathfrak{A}$.

(ii) If $N \subseteq A$, $<$ is a relation on A , and $S : N \rightarrow N$ such that $\langle N, <, S \rangle \cong \langle \omega, <, S \rangle$ and N , $<$ and the graph of S are existentially definable over $\mathfrak{A}$, then $\text{IND}(\exists - \mathfrak{A})$ is $\forall^n_{<}$ -closed for $n > 0$ where

$$\forall^n_{<}(R) = \{(a, \bar{b}) \in A^{n+1} \mid a \in N \ \& \ \forall x (x < a \rightarrow R(x, \bar{b}))\} \quad \text{for } R \subseteq A^{n+1}.$$

PROOF. (i) This is an application of Proposition 3.1.4.

(ii) Let $R = \tau^{-1}\varphi^\infty$ where $\tau : A^{n+1} \rightarrow A^m$ is a section map and $\varphi : \text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$ is positive existential over $\mathfrak{A}$. We show that $\forall^n_{<}(R)$ is in $\text{IND}(\exists - \mathfrak{A})$. First identify N with $\omega = \{0, 1, \dots\}$. Let $\tau_i : A^m \rightarrow A^{m+1}$ be the section maps $\tau_i(\bar{x}) = (i, \bar{x})$ for $\bar{x} \in A^m$ where $i = 0, 1$. Let $\psi(X) = \tau_0\varphi(\tau_0^{-1}X) \cup (\tau_1\tau)\theta((\tau_0\tau)^{-1}X, (\tau_1\tau)^{-1}X)$ for $X \subseteq A^m$, where

$$\theta(Y, Z) = \{(x, \bar{x}) \in A^{n+1} \mid x = 0 \vee \exists y (x = s(y) \ \& \ Y(y, \bar{x}) \ \& \ Z(y, \bar{x}))\}$$

$$\text{for } Y, Z \subseteq A^{n+1}.$$

Then ψ is positive existential over $\mathfrak{A}$. Clearly $\tau_0^{-1}\psi^\infty = \varphi^\infty$. So $R = (\tau_0\tau)^{-1}\psi^\infty$. Hence if $S = (\tau_1\tau)^{-1}\psi^\infty$, then $S(x, \bar{x}) \Leftrightarrow x = 0$ or $\exists y (x = s(y) \ \& \ R(y, \bar{x}) \ \& \ S(y, \bar{x}))$. This can only hold if $S = \forall^n_{<}(R)$. Hence $\forall^n_{<}(R) = (\tau_1\tau)^{-1}\psi^\infty$ is in $\text{IND}(\exists - \mathfrak{A})$. $\square$

3.2.3. PROPOSITION. If $\varphi : \text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$ is positive existential over $\mathfrak{A}$, then $I(\varphi)$ is $T(\mathfrak{A})$ -represented by $\psi(X) \rightarrow X(\bar{x})$, where $\psi(X)$ is $\forall \bar{y} (\varphi(X, \bar{y}) \rightarrow X(\bar{y}))$ where $\varphi(X, \bar{x})$ is an existential formula of $L(\mathfrak{A})$ positive in X that defines the operator.

PROOF. Let T be the relation represented by $\psi(X) \rightarrow X(\bar{x})$. First note that if $\bar{a} \in T$, then by Proposition 2.3.6, $\psi(X) \rightarrow X(\bar{a})$ is universally valid, i.e. $a \in \bigcap \{S \subseteq A^m \mid \varphi(S) \subseteq S\} = I(\varphi)$. Thus $T \subseteq I(\varphi)$. To show $I(\varphi) \subseteq T$ it suffices to show that $\varphi(T) \subseteq T$. We need the following.

Claim. Let $\theta(X)$ be an existential formula of $L(\mathfrak{A})$ containing x only positively and containing no other variables free. Then

$$\theta(T) \text{ is true} \quad \text{implies} \quad T(\mathfrak{A}) \vdash \psi(X) \rightarrow \theta(X).$$

This claim is proved by an easy induction on the number of logical symbols in $\theta(X)$.

Now if $\bar{a} \in \varphi(T)$, then $\varphi(T, \bar{a})$ is true, and hence by the claim $T(\mathfrak{A}) \vdash \psi(X) \rightarrow \varphi(x, \bar{a})$. Recalling that $\psi(X)$ is $\forall \bar{y} (\varphi(X, \bar{y}) \rightarrow X(\bar{y}))$ it follows that $T(\mathfrak{A}) \vdash \psi(X) \rightarrow X(\bar{a})$ and hence $\bar{a} \in T$. Thus $\varphi(T) \subseteq T$ as required. $\square$

3.2.4. THEOREM. *Let $\mathfrak{A}$ be an existentially acceptable structure. Then the following are equivalent for a relation R on A .*

- (i) $R \in \text{IND}(\exists - \mathfrak{A})$,
- (ii) R is $T(\mathfrak{A})$ -representable,
- (iii) R is $\Sigma_1^0(\mathfrak{A})$ -definable.

Note. In (iii), $\Sigma_1^0(\mathfrak{A})$ is defined relative to the copy $\langle N, < \rangle$ of $\langle \omega, < \rangle$ where $\mathcal{C} = \langle N, <, \langle \rangle \rangle$ is an existentially definable coding scheme over $\mathfrak{A}$. It follows from the theorem that $\Sigma_1^0(\mathfrak{A})$ is essentially independent of the coding scheme $\mathcal{C}$ used.

PROOF. (i) $\rightarrow$ (ii). Let $R = \tau^{-1} \varphi^\infty$ where τ is a section map $\tau(\bar{a}) = (\bar{b}, \bar{a})$ for $\bar{a} \in A^n$, and φ is a positive existential operator over $\mathfrak{A}$. Then by Proposition 3.2.3, φ^∞ is $T(\mathfrak{A})$ -representable by a formula $\theta(y)$ say. Then

$$R(\bar{a}) \Leftrightarrow \tau(\bar{a}) \in \varphi^\infty \Leftrightarrow T(\mathfrak{A}) \vdash \theta(\bar{b}, \bar{a}) \quad \text{for } \bar{a} \in A^n,$$

Hence R is $T(\mathfrak{A})$ -represented by $\theta(\bar{b}, \bar{x})$.

(ii) $\rightarrow$ (iii). This is just Corollary 2.3.5.

(iii) $\rightarrow$ (i). This follows from Proposition 3.2.2. $\square$

The following property holds for the r.e. relations on ω and is one of the basic structural properties used in recursion theory and its generalizations.

3.2.5. DEFINITION. A class Γ of relations on A has the *parametrization property* if for each $n > 0$ there is a relation $U \subseteq A^{n+1}$ such that $U \in \Gamma$ and for each $R \subseteq A^n$ that is in Γ there is an $a \in A$ such that

$$R = U_a = \{\bar{a} \in A^n \mid U(a, \bar{a})\}.$$

3.2.6. THEOREM. *If $\mathfrak{A}$ is existentially acceptable, then $\text{IND}(\exists - \mathfrak{A})$ has the parametrization property.*

PROOF. By Corollary 2.3.5 and Theorem 3.2.4 the set $\ulcorner T(\mathfrak{A}) \urcorner$ is in $\text{IND}(\exists - \mathfrak{A})$. We also need the following fact about coding the syntax of $\ulcorner T(\mathfrak{A}) \urcorner$.

The relation Sub is in $\Sigma_1^0(\mathfrak{A})$ and hence in $\text{IND}(\exists - \mathfrak{A})$, where for $a, b, c \in A$ $\text{Sub}(a, b, c) \Leftrightarrow$ there is an elementary formula $\theta(\bar{x})$ in $L(\mathfrak{A})$ with $a = \ulcorner \theta(\bar{x}) \urcorner$ and there is $\bar{b}$ such that $b = \langle \bar{b} \rangle$ and $c = \ulcorner \theta(\bar{b}) \urcorner$.

Now, given $n > 0$ let $U \subseteq A^{n+1}$ be given by

$$U(a, \bar{a}) \Leftrightarrow \exists x [\text{Sub}(a, \langle \bar{a} \rangle, x) \ \& \ x \in \ulcorner T(\mathfrak{A}) \urcorner].$$

Using the closure properties of $\text{IND}(\exists - \mathfrak{A})$ we see that $U \in \text{IND}(\exists - \mathfrak{A})$. Now if $R \subseteq A^n$ is in $\text{IND}(\exists - \mathfrak{A})$ then by 3.2.4, it is $T(\mathfrak{A})$ -represented by a formula $\theta(\bar{x})$ say. Let $a = \ulcorner \theta(\bar{x}) \urcorner$. Then for $\bar{a} \in A^n$

$$\begin{aligned} R(\bar{a}) &\Leftrightarrow \ulcorner \theta(\bar{a}) \urcorner \in T(\mathfrak{A}) \\ &\Leftrightarrow U(a, \bar{a}). \end{aligned}$$

Hence $R = U_a$. $\square$

3.3. Positive elementary induction

In this subsection we will outline some of the properties of positive elementary induction. The theory has been presented in MOSCHOVAKIS [1974a] and readers should look there for a detailed development of the subject.

If $\mathcal{F}$ is the class of elementary formulae of L^A , then we shall write $\text{IND}(\mathfrak{A})$ for $\text{IND}(\text{pos-}\mathcal{F}(\mathfrak{A}))$ and $\kappa(\mathfrak{A})$ for $|\text{pos-}\mathcal{F}(\mathfrak{A})|$.

3.3.1. PROPOSITION. *$\text{IND}(\mathfrak{A})$ is positive elementary closed over $\mathfrak{A}$ (i.e. if θ is section codable in the class of positive elementary operations, then $\text{IND}(\mathfrak{A})$ is closed under θ). Hence the relations $=$, $R_1, \dots, R_l$ and their complements are in $\text{IND}(\mathfrak{A})$ and $\text{IND}(\mathfrak{A})$ is closed under $\vee^n$, $\wedge^n$, $\exists^n$ and $\forall^n$ for $n > 0$.*

This is an application of Proposition 3.1.4.

3.3.2. PROPOSITION. *Let Φ be a rule set on A that is regular elementary over $\mathfrak{A}$. Let $\varphi : \text{Pow}(A) \rightarrow \text{Pow}(A)$ be the associated monotone operator. Then φ is positive elementary over $\mathfrak{A}$ and hence $I(\Phi) = I(\varphi) \in \text{IND}(\mathfrak{A})$.*

PROOF. Let Φ be the set of rules $R_a \rightarrow b$ such that $S(a, b)$. Then for $X \subseteq A$,

$$\varphi(X) = \{b \in A \mid \exists y [S(y, b) \wedge \forall x (R(a, x) \rightarrow X(x))]\}.$$

If R and S are replaced by their elementary definitions then we obtain an elementary definition of φ . $\square$

3.3.3. COROLLARY. *If $\mathfrak{A}$ is acceptable, then $\ulcorner T_{\infty}(\mathfrak{A}) \urcorner \in \text{IND}(\mathfrak{A})$ and hence every $T_{\infty}(\mathfrak{A})$ -representable relation is in $\text{IND}(\mathfrak{A})$.*

PROOF. The first part follows from Propositions 3.3.2 and 2.3.10. The last part is proved as in the last part of Corollary 2.3.5 using some of the closure properties of $\text{IND}(\mathfrak{A})$ given in 3.3.1. $\square$

3.3.4. PROPOSITION. *If $\varphi : \text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$ is positive elementary over $\mathfrak{A}$, then $I(\varphi)$ is $T_{\infty}(\mathfrak{A})$ -representable.*

PROOF. This result is proved as in the proof of Proposition 3.2.3. The claim used there must be modified by replacing $T(\mathfrak{A})$ by $T_{\infty}(\mathfrak{A})$ and allowing $\theta(X)$ to be any elementary formula of $L(\mathfrak{A})$. The A -rule of $T_{\infty}(\mathfrak{A})$ is just what is needed in order to take care of the proof for the case that $\theta(X)$ is a universal quantification. $\square$

As a consequence of the previous two results we have:

3.3.5. THEOREM. *For acceptable $\mathfrak{A}$ and relation R on A , $R \in \text{IND}(\mathfrak{A})$ iff R is $T_{\infty}(\mathfrak{A})$ -representable.*

As in the proof of Theorem 3.2.6, we have:

3.3.6. COROLLARY. *If $\mathfrak{A}$ is acceptable, then $\text{IND}(\mathfrak{A})$ has the parametrization property.*

The following result is called the Abstract Kleene Theorem in MOSCHOVAKIS [1974a]. The proof given there uses a quite different method to the one we use.

3.3.7. THEOREM. *If $\mathfrak{A}$ is a countable acceptable structure and R is a relation on A , then $R \in \text{IND}(\mathfrak{A})$ iff R is $\Pi_1^1(\mathfrak{A})$.*

This theorem is an immediate consequence of Corollary 2.3.8 and Theorem 3.3.5.

3.3.8. DEFINITION. A *norm* on a set R is a map $\sigma : R \rightarrow \lambda$ of R onto an ordinal λ . λ is called the *length* of σ .

If $R \subseteq A^n$ then associated with σ are the $2n$ -ary relations $<_{\sigma}^*$ and $\leq_{\sigma}^*$ given by

$$\bar{a} <_{\sigma}^* \bar{b} \Leftrightarrow R(\bar{a}) \ \& \ (R(\bar{b}) \Rightarrow \sigma(\bar{a}) < \sigma(\bar{b})),$$

$$\bar{a} \leq_{\sigma}^* \bar{b} \Leftrightarrow R(\bar{a}) \ \& \ (R(\bar{b}) \Rightarrow \sigma(\bar{a}) \leq \sigma(\bar{b})),$$

for $\bar{a}, \bar{b} \in A^n$.

3.3.9. EXAMPLE. If $\varphi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$, then $|\varphi : \varphi^\infty \rightarrow \varphi|$ is a norm on φ^∞ . We write $<_{\varphi}^*$ and $\leq_{\varphi}^*$ rather than $<_{\sigma}^*$ and $\leq_{\sigma}^*$ when $\sigma = |\varphi|$.

3.3.10. DEFINITION. Let Γ be a class of relations on A . If R is a relation on A , then a norm σ on R is a Γ -norm if $<_{\sigma}^*$ and $\leq_{\sigma}^*$ are in Γ . Γ is *normed* if every relation in Γ has a Γ -norm. For normed Γ let $\text{o}(\Gamma)$ be the supremum of the lengths of the Γ -norms.

3.3.11. PROPOSITION. $\text{IND}(\mathfrak{U})$ is *normed*.

PROOF. Let $R = \tau^{-1}\varphi^\infty$ where τ is a section map and φ is positive elementary over $\mathfrak{U}$. Let $\sigma_0(\bar{a}) = |\tau(\bar{a})|_{\varphi}$ for $\bar{a} \in R$. $\sigma_0 : R \rightarrow |\varphi|$ may not be a norm as its range may not be an initial segment of ordinals. But there is a unique order preserving function f mapping the range of σ_0 onto an ordinal λ . Then if $\sigma(\bar{a}) = f(\sigma_0(\bar{a}))$ for $\bar{a} \in R$, $\sigma : R \rightarrow \lambda$ is a norm on R of length $\lambda \searrow |\varphi|$.

Note that for $\bar{a}, \bar{b} \in A^n$, $\bar{a} <_{\sigma}^* \bar{b}$ iff $\tau(\bar{a}) <_{\varphi}^* \tau(\bar{b})$ and similarly for $\leq_{\sigma}^*$. Hence to prove the proposition it suffices to show that $<_{\varphi}^*$ and $\leq_{\varphi}^*$ are in $\text{IND}(\mathfrak{U})$. This follows from:

3.3.12. FIRST STAGE COMPARISON THEOREM. Let $\varphi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ be a positive elementary operator. Then there are positive elementary operators $\varphi_{<}, \varphi_{\leq} : \text{Pow}(A^{2n}) \rightarrow \text{Pow}(A^{2n})$ such that

$$<_{\varphi}^* = I(\varphi_{<}) \quad \text{and} \quad \leq_{\varphi}^* = I(\varphi_{\leq}).$$

Moreover, $\varphi_{<}(X) = \{(\bar{a}, \bar{b}) \in A^{2n} \mid (\bar{b}, \bar{a}) \in \varphi_{\leq}(X)\}$ for $X \subseteq A^{2n}$.

PROOF. $\varphi_{<}$ and $\varphi_{\leq}$ are defined as follows. Let

$$\theta(X) = \{(\bar{a}, \bar{b}) \in A^{2n} \mid \bar{a} \in \varphi'(\{x \in A^n \mid (\bar{b}, \bar{x}) \in X\})\} \quad \text{for } X \subseteq A^{2n},$$

where $\varphi'(Y) = \varphi(Y) \cup Y$ for $Y \subseteq A^n$. Then let $\varphi_{\leq}(X) = \theta(\check{\theta}(X))$ for $X \subseteq A^{2n}$ and define $\varphi_{<}$ as required by the theorem. Then observe that θ is positive elementary and hence that $\varphi_{\leq}$ and $\varphi_{<}$ are also. The proof that these operators inductively define $\leq_{\varphi}^*$ and $<_{\varphi}^*$ follows easily from the lemma below. $\square$

3.3.13. LEMMA. *For all ordinals λ ,*

$$\bar{a} <_{\varphi}^* \bar{b} \ \& \ \bar{a} \in \varphi^{\lambda} \Leftrightarrow (\bar{a}, \bar{b}) \in \varphi_{<}^{\lambda},$$

$$\bar{a} \leq_{\varphi}^* \bar{b} \ \& \ \bar{a} \in \varphi^{\lambda} \Leftrightarrow (\bar{a}, \bar{b}) \in \varphi_{\leq}^{\lambda}.$$

PROOF. This lemma is proved by induction on λ . $\square$

3.3.14. DEFINITION. A relation R on A such that both R and $\neg R$ are in $\text{IND}(\mathfrak{A})$ is called *hyperelementary over $\mathfrak{A}$* . We write $\text{HYP}(\mathfrak{A})$ for the class of such relations.

This class generalizes the class of hyperarithmetical relations on ω .

3.3.15. COROLLARY. *If $\varphi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ is positive elementary over $\mathfrak{A}$, then $\varphi^{\lambda} \in \text{HYP}(\mathfrak{A})$ for all $\lambda < |\varphi|$.*

PROOF. If $\lambda < |\varphi|$, then $\lambda = |\bar{a}|_{\varphi}$ for some $\bar{a} \in I(\varphi)$. So

$$\varphi^{\lambda} = \{x \in A^n \mid x \leq_{\varphi}^* a\} = \{x \in A^n \mid (x, a) \in \varphi_{\leq}^{\infty}\} = \{\bar{x} \in A^n \mid (\bar{a}, \bar{x}) \in \check{\varphi}_{\leq}^{\infty}\},$$

$$\neg \varphi^{\lambda} = \{\bar{x} \in A^n \mid \bar{a} <_{\varphi}^* \bar{x}\} = \{\bar{x} \in A^n \mid (\bar{a}, \bar{x}) \in \varphi_{<}^{\infty}\}.$$

So if $\tau(\bar{x}) = (\bar{a}, \bar{x})$ for $\bar{x} \in A^n$, then

$$\varphi^{\lambda} = \tau^{-1} \check{\varphi}_{\leq}^{\infty} \quad \text{and} \quad \neg \varphi^{\lambda} = \tau^{-1} \varphi_{<}^{\infty}.$$

Hence $\varphi^{\lambda} \in \text{HYP}(\mathfrak{A})$. $\square$

The basic properties of the Π_1^1 relations on ω , and more generally of $\text{IND}(\mathfrak{A})$ for $\mathfrak{A}$ an acceptable structure, are incorporated in the following important definition first introduced in MOSCHOVAKIS [1974a].

3.3.16. DEFINITION. A class Γ of relations on a set A is a *Spector class over $\mathfrak{A}$* if

- (i) Γ is positive elementary closed over $\mathfrak{A}$ (see Proposition 3.3.1),
- (ii) Γ contains a coding scheme $\mathcal{C}$ on A (i.e. N , $\leq$, Seq, the graphs of lh, q and s and the complements of all these are in Γ where these are defined in Definition 2.3.2),
- (iii) Γ has the parametrization property (see Definition 3.2.5),
- (iv) Γ is normed.

3.3.17. THEOREM. *If $\mathfrak{A}$ is an acceptable structure, then $\text{IND}(\mathfrak{A})$ is the smallest Spector class over $\mathfrak{A}$.*

This result also holds under the slightly weaker hypothesis that $\mathfrak{A}$ is *almost acceptable*, where this means that $\text{IND}(\mathfrak{A})$ contains a coding scheme on A . The fact that $\text{IND}(\mathfrak{A})$ is a Spector class over $\mathfrak{A}$ is obtained by combining Proposition 3.3.1 and 3.3.12, and Corollary 3.3.6. To see that it is the smallest one requires the following result about Spector classes.

3.3.18. THEOREM. *Let Γ be a Spector class over $\mathfrak{A}$. Let $\varphi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ be positive elementary over $\mathfrak{A}$. Then $I(\varphi) \in \Gamma$.*

PROOF. We sketch a proof of this. The details may be found in 9A of MOSCHOVAKIS [1974a]. By the parametrization property of Γ choose $U \subseteq A^{n+2}$ in Γ to parametrize the $(n+1)$ -ary relations in Γ . Let $\tau : U \rightarrow \kappa$ be a Γ -norm on U . Let $Q(t, \bar{a}) \Leftrightarrow \bar{a} \in \varphi(\{\bar{x} \in A^n \mid (t, t, \bar{x}) <^*_\tau(t, t, \bar{a})\})$. Then as Γ is positive elementary closed $Q \in \Gamma$ and hence $Q = U_a$ for some $a \in A$.

Let $P(\bar{a}) \Leftrightarrow Q(a, \bar{a})$ for $\bar{a} \in A^n$. Let $\sigma_0 : P \rightarrow \kappa$ be given by $\sigma_0(\bar{a}) = \tau(a, a, \bar{a})$ for $a \in P$. σ_0 may not be surjective, but by composing with an order preserving mapping of the range of σ_0 onto an initial segment of ordinals we obtain a norm σ on P . Then for $a \in A^n$,

$$P(\bar{a}) \Leftrightarrow \bar{a} \in \varphi(\{\bar{x} \in A^n \mid \bar{x} <^*_\sigma \bar{a}\}).$$

But it may easily be shown that any P with a norm satisfying this equivalence must be identical with $I(\varphi)$. Hence as $P \in \Gamma$, $I(\varphi) \in \Gamma$. $\square$

The ordinal $\kappa(\mathfrak{A})$ may be characterised in terms of $\text{IND}(\mathfrak{A})$ as the sup of the lengths of the positive elementary inductive norms over $\mathfrak{A}$, i.e.:

3.3.19. THEOREM. $\kappa(\mathfrak{A}) = o(\text{IND}(\mathfrak{A}))$.

The next result generalizes the Spector–Gandy theorem for the Π^1_1 relations on ω .

3.3.20. ABSTRACT SPECTOR–GANDY THEOREM. *Let $\mathfrak{A}$ be an acceptable structure. If $R \subseteq A^n$, then $R \in \text{IND}(\mathfrak{A})$ iff there is an elementary second order relation $\mathcal{R}$ such that for $\bar{a} \in A^n$*

$$R(\bar{a}) \Leftrightarrow \exists X \in \text{HYP}(\mathfrak{A}) \mathcal{R}(X, \bar{a}).$$

This result was first stated and proved in MOSCHOVAKIS [1974a]. A simplification of that proof was given in ACZEL [1972]. It used a new proof

of Moschovakis's second stage comparison theorem (7 C.1. of MosCHOVAKIS [1974a]). The following consequence is the main fact needed.

3.3.21. PROPOSITION. *Let $\varphi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ be positive elementary over $\mathfrak{A}$. Then there is a second order relation $\mathcal{Q}$ that is elementary over $\mathfrak{A}$ such that if $\bar{a} \in I(\varphi)$ or $\bar{b} \in I(\varphi)$, then the following are equivalent*

- (i) $\bar{a} \leq_\varphi^* \bar{b}$,
- (ii) $\exists X \mathcal{Q}(X, \bar{a}, \bar{b})$,
- (iii) $\exists X \in \text{Hyp}(\mathfrak{A}) \mathcal{Q}(X, \bar{a}, \bar{b})$.

PROOF. Let $\varphi_\leq : \text{Pow}(A^{2^n}) \rightarrow \text{Pow}(A^{2^n})$ be the operator used in the First Stage Comparison Theorem 3.3.12. Let $\mathcal{Q}(X, \bar{a}) \Leftrightarrow \bar{a} \in X \ \& \ X \subseteq \varphi_\leq(X)$, for $X \subseteq A^{2^n}$ and $\bar{a} \in A^{2^n}$. Then $\mathcal{Q}$ is elementary over $\mathfrak{A}$. To see that (i) and (ii) are equivalent,

$$\begin{aligned} \bar{a} \leq_\varphi^* \bar{b} &\Leftrightarrow \neg \bar{b} <_\varphi^* \bar{a} \Leftrightarrow (\bar{b}, \bar{a}) \notin \varphi_\leq^* \Leftrightarrow (\bar{a}, \bar{b}) \notin (\varphi_\leq^*)^\circ \\ &\Leftrightarrow \neg \forall Y [\check{\varphi}_\leq(Y) \subseteq Y \Rightarrow Y(\bar{a}, \bar{b})] \\ &\Leftrightarrow \exists X [\check{\varphi}_\leq(\neg X) \subseteq \neg X \ \& \ X(\bar{a}, \bar{b})] \Leftrightarrow \exists X \mathcal{Q}(X, \bar{a}, \bar{b}). \end{aligned}$$

As (iii) $\Rightarrow$ (ii) is trivial it only remains to show that (i) $\Rightarrow$ (iii). So let $\bar{a} \leq_\varphi^* \bar{b}$. Then for some $\lambda < |\varphi|$, $\bar{a} \in \varphi^\lambda$ and hence by Definition 3.3.13, $(\bar{a}, \bar{b}) \in \varphi_\leq^\lambda$. As $\varphi_\leq^\lambda \subseteq \varphi(\varphi_\leq^\lambda)$ it follows that $\mathcal{Q}(\varphi_\leq^\lambda, \bar{a}, \bar{b})$. As $\lambda < |\varphi| = |\varphi_\leq|$ it follows from Corollary 3.3.15 that $\varphi_\leq^\lambda \in \text{HYP}(\mathfrak{A})$. Hence $\exists X \in \text{HYP}(\mathfrak{A}) \mathcal{Q}(X, \bar{a}, \bar{b})$. $\square$

We end this outline of the theory of positive elementary induction by giving, without proof, Moschovakis's normal form theorem for an acceptable structure. For this we need to introduce the game quantifier.

In general, by a *quantifier* on a set A we mean a set $Q \subseteq \text{Pow}(A)$. If $R \subseteq A$ we write $Qz R(z)$ instead of $R \in Q$. For example the existential and universal quantifiers on A are $\exists = \text{Pow}(A) - \{\emptyset\}$ and $\forall = \{A\}$.

Given an elementary coding scheme for a structure $\mathfrak{A}$ the *game quantifier* G on A is the set of $R \subseteq A$ such that

$$(*) \quad \{\forall x_1 \exists y_1 \forall x_2 \exists y_2 \cdots\} \vee_{m \in \omega} R(\langle x_1, y_1, \dots, x_m, y_m \rangle).$$

Eq. (*) is interpreted in the usual way in terms of a game $\mathcal{G}(R)$ between two players $\exists$ and $\forall$ who alternately choose elements of A , starting with $\forall$, to produce a sequence $x_1, y_1, x_2, y_2, \dots$. If for some m , $\langle x_1, y_1, \dots, x_m, y_m \rangle \in R$, then player $\exists$ wins. If this never happens then player $\forall$ wins. Now (*) is

interpreted to mean that player $\exists$ has a winning strategy for the game $\mathcal{G}(R)$.

3.3.22. THEOREM (5C of MOSCHOVAKIS [1974a]). *Let $\mathfrak{A}$ be an acceptable structure. Let G be the game quantifier on A relative to an elementary coding scheme for $\mathfrak{A}$. Then for $R \subseteq A^n$, $R \in \text{IND}(\mathfrak{A})$ iff there is an elementary relation $S \subseteq A^{n+1}$ such that for $\bar{a} \in A^n$,*

$$R(\bar{a}) \Leftrightarrow Gz S(z, \bar{a}).$$

3.4. Relativisation to a non-trivial monotone quantifier

In this subsection we indicate how the notions and results of the last section can be generalised by relativising to a non-trivial monotone quantifier Q on A . $Q \subseteq \text{Pow}(A)$ is *non-trivial* if $Q \neq \emptyset$ and $Q \neq \text{Pow}(A)$. Q is *monotone* if $A \supseteq X \supseteq Y \in Q$ implies $X \in Q$. The quantifier $\check{Q}$ *dual* to Q is given by $\check{Q}z R(z) \Leftrightarrow \neg Qz \neg R(z)$. The language $L^A(Q)$ is defined like L^A except that formulae $Qz \phi(z)$ and $\check{Q}z \phi(z)$ are allowed for any formula $\phi(z)$.

The standard interpretation of L^A is extended to sentences of $L^A(Q)$ by requiring that

$$Qx \phi(x) \text{ is true} \quad \text{iff} \quad \{a \in A \mid \phi(a) \text{ is true}\} \in Q,$$

and similarly for $\check{Q}x \phi(x)$.

The language $L(\mathfrak{A}, Q)$ is the sublanguage of $L^A(Q)$ corresponding to the sublanguage $L(\mathfrak{A})$ of L^A . Positive and negative occurrences of relations in a formula of $L^A(Q)$ are defined by treating Q and $\check{Q}$ in the same way as the ordinary quantifiers. Define the *Q-elementary* formulae of $L^A(Q)$ like the elementary formulae of L^A except that Qx and $\check{Q}x$ are allowed. Now define $\text{IND}(\mathfrak{A}, Q)$ as in the definition of $\text{IND}(\mathfrak{A})$ except using positive Q -elementary operators instead of the positive elementary ones.

Now the result of 3.3 concerning $\text{IND}(\mathfrak{A})$ will carry over to $\text{IND}(\mathfrak{A}, Q)$ with suitable changes, i.e. “elementary” should be replaced by “ Q -elementary”. Where $\mathfrak{A}$ is required to be acceptable, it is sufficient here that $\mathfrak{A}$ is Q -acceptable, i.e. there is a Q -elementary coding scheme. Among the positive Q -elementary operators there are the Q^n and $\check{Q}^n$ defined like $\forall^n$ and $\exists^n$. The theory $T_\infty(\mathfrak{A})$ needs to be replaced by the theory $T_\infty(\mathfrak{A}, Q)$. This is obtained from $T_\infty(\mathfrak{A})$ by allowing Q -elementary formulae and adding the following possibly infinitary rules.

Q-rule: From $\theta(a)$ for $a \in X$ infer $Qx \theta(x)$ if $X \in Q$.

$\check{Q}$ -rule: From $\theta(a)$ for $a \in X$ infer $\check{Q}x \theta(x)$ if $X \in \check{Q}$.

(See ACZEL [1970] where such rules are considered.) Using $T_\infty(\mathfrak{A}, Q)$, results 3.3.3–3.3.6 carry over to $\text{IND}(\mathfrak{A}, Q)$. There does not seem to be any analogue of Theorem 3.3.7. Theorem 3.3.17 carries over to yield that if $\mathfrak{A}$ is Q -acceptable then $\text{IND}(\mathfrak{A}, Q)$ is the smallest Spector class over $\mathfrak{A}$ that is closed under each Q^n and $\check{Q}^n$.

The Abstract Spector–Gandy Theorem 3.3.20 also carries over to $\text{IND}(\mathfrak{A}, Q)$. Of course $\text{HYP}(\mathfrak{A}, Q)$ must be used instead of $\text{HYP}(\mathfrak{A})$.

The Normal Form Theorem 3.3.22 also carries over, but for this it is necessary to generalise the game quantifier. This has been carried out in ACZEL [1975] where it is shown how to interpret any infinite string $Q_1x_1Q_2x_2\cdots$ of non-trivial monotone quantifiers as the following alternating string of ordinary quantifiers:

$$\exists X_1 \in Q_1 \forall x_1 \in X_1 \exists X_2 \in Q_2 \forall x_2 \in X_2 \cdots$$

This can be interpreted in terms of a game between two players as in the definition of the game quantifier. Now given a Q -elementary coding scheme for the structure $\mathfrak{A}$ we define the relativisation Q^+ of the game quantifier as the set of $R \subseteq A$ such that

$$\{Qx_1 \check{Q}y_1 \forall x_2 \exists y_2 Qx_3 \check{Q}y_3 \cdots\} \vee_{m \in \omega} R(\langle x_1, y_1, \dots, x_m, y_m \rangle).$$

Note that $\forall^+$ is just the game quantifier G . Theorem 3.3.22 carries over to $\text{IND}(\mathfrak{A}, Q)$ if G is replaced by Q^+ .

We end this section by stating an important recently obtained result.

3.4.1. THEOREM (HARRINGTON [1975]). *Let $\mathfrak{A}$ be an acceptable structure. Every Spector class over $\mathfrak{A}$ has the form $\text{IND}(\mathfrak{A}, Q)$ for some non-trivial monotone quantifier Q on A .*

3.5. Non-monotone induction

The first examples of non-monotone inductive definitions were those that appeared in the construction of various systems of notations for larger and larger segments of the countable ordinals. The first such systems were those of Church–Kleene for the recursive ordinals. One such example is Kleene's $\mathcal{O}$ considered in 2.2. The first ordinal not having a notation in $\mathcal{O}$ is the Church–Kleene ordinal ω_1 , that is a recursive analogue of the first uncountable ordinal. The inductive definition of $\mathcal{O}$ uses a monotone operator. But attempts to extend $\mathcal{O}$ to systems of notations for recursive analogues of the higher number classes soon lead to non-monotone operators. For example let $\phi : \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ be the monotone

operator associated with the regular arithmetical rule set generating Kleene's $\mathcal{O}$ in 2.2. We may extend $\mathcal{O}$ by adding a notation 7 (say) for the ordinal ω , and then continuing as before, i.e. we define a non-monotone operator $\phi_1: \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ given by

$$\phi_1(X) = \begin{cases} \phi(X) & \text{if } \phi(X) \not\subseteq X, \\ \{7\} & \text{if } \phi(X) \subseteq X \end{cases} \quad \text{for } X \subseteq \omega.$$

Then for $\lambda < |\phi| = \omega_1$, $\phi^\lambda_1 = \phi^\lambda$ so that $\phi^{\omega_1}_1 = \phi^{<\omega_1} \cup \{7\} = \mathcal{O} \cup \{7\}$. Hence $|7|_{\phi_1} = \omega_1$. It is not hard to see that $|\phi_1| = \omega_1 + \omega_1$ so that ϕ^∞_1 is a set of notations for the ordinals $< \omega_1 + \omega_1$. The above may be continued very much further and leads to notation systems for much larger ordinals such as recursive analogues of the finite and transfinite number classes. (See ADDISON and KLEENE [1957], KREIDER and ROGERS [1961], PUTNAM [1961] and RICHTER [1965, 1967, 1968].)

The above work was concerned with the details of specific notation systems. In PUTNAM [1964] a more general approach was taken where it was shown that arbitrary Δ^1_2 inductive definitions can only give notation systems for an initial segment of the Δ^1_2 ordinals (i.e. the order types of Δ^1_2 well-orderings of natural numbers). Further work has shifted the interest from the study of specific inductively defined notation systems to the study of classes $\mathcal{E}$ of inductive definitions on ω , and the associated ordinals $|\mathcal{E}|$. This shift, encouraged by Gandy, led to the work of RICHTER [1971], ACZEL and RICHTER [1972], RICHTER and ACZEL [1974], AANDERAA [1974], CENZER [1974] and RICHTER [1976]. This work gives characterisations of $|\mathcal{E}|$, for various classes $\mathcal{E}$, in terms of recursive analogues of large cardinals. Such analogues were defined using Kripke's theory of recursion on admissible ordinals. The starting point is to take the admissible ordinals as the recursive analogue of the regular ordinals. It turns out that the first admissible $> \omega$ is the Church-Kleene ordinal ω_1 so that the two approaches to recursive analogues agree. Other analogues are the recursive inaccessible (admissible limits of admissible ordinals) and the recursively Mahlo ordinals (admissibles α such that for every α -recursive $f: \alpha \rightarrow \alpha$ there is an admissible $\beta < \alpha$ closed under f). For recursive analogues of even larger cardinals reflection properties were introduced in RICHTER and ACZEL [1974]. Examples are the Π^0_{n+2} -reflecting ordinals which give a recursive analogue for the Π^1_n -inaccessible cardinals for $n > 0$.

Below we shall state some of the results obtained. But first we need a construction invented in RICHTER [1971]. Given $\phi, \psi: \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ define $[\phi, \psi]: \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ by

$$[\phi, \psi](X) = \begin{cases} \phi(X) & \text{if } \phi(X) \not\subseteq X, \\ \psi(X) & \text{if } \phi(X) \subseteq X \end{cases} \quad \text{for } X \subseteq \omega.$$

Note that ϕ_1 introduced above is $[\phi, \psi]$ where $\psi(X) = \{7\}$ for all $X \subseteq \omega$. If $\mathcal{E}_1, \mathcal{E}_2$ are classes of operators on ω let $[\mathcal{E}_1, \mathcal{E}_2] = \{[\phi_1, \phi_2] \mid \phi_1 \in \mathcal{E}_1 \text{ and } \phi_2 \in \mathcal{E}_2\}$.

3.5.1. PROPOSITION. (i) $|\Pi_0^0| = \omega$.

(ii) (Gandy, unpublished) $|\Pi_1^0| = \omega_1$.

(iii) (PUTNAM [1964]) $|\Delta_2^1| = \delta_2^1$, *the first non Δ_2^1 ordinal*.

(iv) (RICHTER [1971]) $|\Pi_0^0, \Pi_0^0| = \omega^2$, $|\Pi_1^0, \Pi_1^0| = \text{first recursive inaccessible}$, $|\Pi_1^0, \Pi_1^0| = \text{first recursively Mahlo ordinal}$.

(v) (ACZEL and RICHTER [1972]) $|\Pi_n^0| = |\Sigma_{n+1}^0| = \text{first } \Pi_{n+1}^0 \text{ reflecting ordinal}$.

(vi) (ACZEL and RICHTER [1972]) $|\Pi_1^1| = \text{first } \Pi_1^1 \text{ reflecting ordinal}$, $|\Sigma_1^1| = \text{first } \Sigma_1^1 \text{ reflecting ordinal}$.

(vii) (RICHTER [1976]) $|\Pi_2^1| = \text{first } \Pi_2^1 \text{ reflecting ordinal}$.

(viii) (AANDERAA [1974]) $|\Pi_1^1| < |\Sigma_1^1|$ and $|\Sigma_2^1| < |\Pi_2^1|$.

Many more results may be found in the above-mentioned papers. It is interesting to compare these results with corresponding results for classes of positive and monotone operators on ω .

3.5.2. PROPOSITION. (i) $|\text{pos-}\Sigma_1^0| = |\text{mon-}\Sigma_1^0| = \omega$.

(ii) (SPECTOR [1961]) $|\text{pos-}\Pi_1^0| = |\text{mon-}\Pi_1^0| = \omega_1$.

(iii) (Grilliot, unpublished) $|\text{pos-}\Sigma_1^1| = |\text{mon-}\Sigma_1^1| = |\Sigma_1^1|$.

(vi) (Gandy, unpublished) $|\text{pos-}\Sigma_2^1| = |\text{mon-}\Sigma_2^1| = \delta_2^1$.

Moschovakis has recently raised the problem of characterising $|\text{pos-}\Pi_2^1| = |\text{mon-}\Pi_2^1|$. It is not even known whether this ordinal is admissible.

In the above we have only stated results about $|\mathcal{E}|$. Of course the class $\text{IND}(\mathcal{E})$ is also of interest. Under general conditions on $\mathcal{E}$ the ordinal $|\mathcal{E}|$ is admissible and $\text{IND}(\mathcal{E})$ is a Spector class with $|\mathcal{E}| = o(\text{IND}(\mathcal{E}))$. Moreover in many cases considered in RICHTER and ACZEL [1974], $\text{IND}(\mathcal{E})$ may be characterized, in terms of α -recursion, as the class of α -r.e. relations on ω where $\alpha = |\mathcal{E}|$.

The theory of non-monotone induction on ω has been most elegantly generalised to abstract structures in MOSCHOVAKIS [1974b]. The central

notion of that paper is that of a *typical, non-monotone* class of second order relations over an abstract structure $\mathfrak{A}$. Examples are the classes of Σ_k^n or Π_k^n definable second order relations over $\mathfrak{A}$ when $m, k \geq 1$ or $m = 0$ and $k \geq 2$. In case $m = 0$ these classes are defined relative to a hyper-elementary coding scheme over $\mathfrak{A}$, as in 2.3.

3.5.3. THEOREM (MOSCHOVAKIS [1974b]). *Let $\mathcal{T}$ be a typical, non-monotone class of second order relations on $\mathfrak{A}$. Let $\mathcal{E}$ be the set of operators $\phi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ such that $\{(\bar{x}, X) \in A^n \times \text{Pow}(A^n) \mid \bar{x} \in \phi(X)\}$ is in $\mathcal{T}$. Then $\text{IND}(\mathcal{E})$ is a Spector class over $\mathfrak{A}$ with $|\mathcal{E}| = o(\text{IND}(\mathcal{E}))$.*

Moschovakis goes on to characterise $\text{IND}(\mathcal{E})$ as the smallest Spector class over $\mathfrak{A}$ satisfying certain additional conditions.

We end this subsection by stating a special case of an interesting general result of HARRINGTON and KECHRIS [1975].

Let $\mathfrak{A}$ be an acceptable structure, and let $\mathcal{E}$ (pos- $\mathcal{E}$, mon- $\mathcal{E}$) be the class of elementary (positive elementary, monotone elementary) operators over $\mathfrak{A}$. Let $\text{WF} = \{S \subseteq A^2 \mid S \text{ is well-founded}\}$.

3.5.4. THEOREM (HARRINGTON and KECHRIS [1975]). *If WF is elementary over $\mathfrak{A}$, then $\text{IND}(\mathcal{E}) = \text{IND}(\text{mon-}\mathcal{E})$.*

This result is in contrast to the situation for countable $\mathfrak{A}$ when $\text{IND}(\text{pos-}\mathcal{E}) = \Pi_1^1(\mathfrak{A}) = \text{IND}(\text{mon-}\mathcal{E})$. ($\text{IND}(\mathcal{E})$ is always very much larger than $\text{IND}(\text{pos-}\mathcal{E})$.)

3.6. Induction and admissible sets

In this subsection we will assume some familiarity with the notion of an admissible set (see Chapter A.7).

Given an admissible set A , let $\mathfrak{A} = \langle A, \in \upharpoonright A \rangle$. The class of Σ_1 formulae of L^A are built up from the atomic formulae and their negations using $\vee$, $\wedge$, $\exists x$ and the restricted universal quantifier $\forall x \in y$. As in 2.3 the Σ_1 relations over $\mathfrak{A}$ are those relations on A definable over A by a Σ_1 formula of $L(\mathfrak{A})$. (Note that this means that constants for elements of A are allowed.) As in 3.1 we define the class of operators $\phi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ that are positive Σ_1 over $\mathfrak{A}$, the ordinal $o(A)$ of A is the smallest ordinal not in A . Finally, recall that a relation $R \subseteq A^n$ is *A-finite* if $R \in A$. (Note that, as A is closed under pairing, $A^n \subseteq A$ for $n > 0$. So every relation on A is a subset of A .) Much of the interest in admissible sets centres around the infinitary languages L_A that are

associated with them. Recall that these are extensions of first order languages where the formulae are set-theoretically represented as elements of A , and infinite conjunctions and disjunctions $\bigwedge \Phi$ and $\bigvee \Phi$ are allowed as long as Φ is an A -finite set of formulae. Just as the syntax of first order languages is full of effectively presented finitary inductive definitions, the syntax of L_A uses the following. Below let A be a fixed admissible set.

3.6.1. DEFINITION. (i) A rule set Φ on A is *A -finitary* if the set of premisses of every rule in Φ is A -finite.

(ii) An A -finitary rule set Φ is Σ_1 over $\mathfrak{A}$ if it is so as a binary relation on A .

The following result essentially generalises Proposition 2.1.2 (in fact 2.1.2 is essentially the special case when A is the set HF of hereditarily finite sets).

3.6.2. PROPOSITION. *If Φ is an A -finitary rule set that is Σ_1 over $\mathfrak{A}$, then $I(\Phi)$ is Σ_1 over $\mathfrak{A}$.*

PROOF. Let $\phi : \text{Pow}(A) \rightarrow \text{Pow}(A)$ be the monotone operator associated with Φ . Let $\text{Pr}_\phi(a, b)$ if $a \in A$ is a ϕ -proof of b (see Definition 1.4.1). Then it follows easily from the assumptions that Pr_ϕ is Σ_1 over $\mathfrak{A}$. Hence it would suffice to show that $I(\Phi) = \{b \in A \mid \exists a \in A \text{Pr}_\phi(a, b)\}$. But the natural proof of this will only work if $\mathfrak{A}$ satisfies “every set can be well-ordered”.

Hence we use a modification of the notion of ϕ -proof. We say that $\{a_\mu\}_{\mu \leq \lambda}$ is a *ϕ -quasi-proof* of b if

(i) $a_\lambda = \{b\}$, and

(ii) $a_\nu \subseteq \phi(\bigcup_{\mu < \nu} a_\mu)$ for all $\nu \leq \lambda$.

As in the proof of Proposition 1.4.2 we can show that for an arbitrary monotone operator

$$(*) \quad I(\phi) = \{a \in A \mid a \text{ has a } \phi\text{-quasi-proof}\}.$$

But the proof of $(*)$ requires no form of the axiom of choice, in contrast to the proof of 1.4.2.

Now let $\text{qPr}_\phi(a, b)$ if $a \in A$ is a ϕ -quasi-proof of b . As qPr_ϕ is easily seen to be Σ_1 over $\mathfrak{A}$ it suffices to prove the

Claim. $I(\Phi) = \{b \in A \mid \exists a \in A \text{qPr}_\phi(a, b)\}$.

The inclusion $\supseteq$ follows from (*) above. For the other inclusion it is sufficient to show that the right-hand side is Φ -closed. So let $\Phi : X \rightarrow b$ such that every element of X has a ϕ -quasi-proof in A , i.e.,

$$\forall x \in X \exists a \in A \text{ qPr}_\phi(a, x).$$

We must find a ϕ -quasi-proof of b in A . As qPr_ϕ is Σ_1 over $\mathfrak{A}$ we may use strong Σ_1 collection to find a set $Y \in A$ such that

$$\forall x \in X \exists a \in Y \text{ qPr}_\phi(a, x)$$

and

$$\forall a \in Y \exists x \in X \text{ qPr}_\phi(a, x).$$

It follows that each $a \in Y$ is a sequence $\{a_\mu\}_{\mu \leq \lambda_a}$. Let λ be the least ordinal such that $\lambda > \lambda_a$ for all $a \in Y$, $c_\lambda = \{b\}$ and $c_\mu = \bigcup \{a_\mu \mid a \in Y \text{ and } \mu \leq \lambda_a\}$ for $\mu < \lambda$. Then as A is an admissible set $\lambda < o(A)$ and $c \in A$. Also, by construction c is a ϕ -quasi-proof of b . Hence $\exists a \in A \text{ qPr}_\phi(a, b)$. $\square$

Note that it follows from the above claim that only ϕ -quasi-proofs $\{a_\mu\}_{\mu \leq \lambda}$ of length $\lambda < o(A)$ are needed. Hence $|\phi| \leq o(A)$.

Remark. The same proof shows that if $\mathfrak{A}$ is a model of ZF, then $I(\Phi)$ is first order definable over $\mathfrak{A}$ whenever Φ is an A -finitary rule set that is first order definable over $\mathfrak{A}$.

There is an approach to Barwise's compactness theorem for L_A , when A is a countable admissible set, that makes use of the class of positive Σ_1 over $\mathfrak{A}$ inductive definitions. This idea was first suggested by Gandy. A version of this approach may be found in ACZEL [1973]. Here we will just consider the following result.

3.6.3. THEOREM (Gandy). *Let $\phi : \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ be positive Σ_1 over $\mathfrak{A}$. Then*

(i) *if $R \subseteq A^n$ is Σ_1 over $\mathfrak{A}$, then $\bar{a} \in \phi(R)$ implies $\bar{a} \in \phi(R')$ for some A -finite $R' \subseteq R$.*

(ii) *$I(\phi)$ is Σ_1 over $\mathfrak{A}$ and $|\phi| \leq o(A)$.*

PROOF. (i) It suffices to show that for each Σ_1 formula $\theta(X)$ of $L(\mathfrak{A})$, containing positive occurrences of the n -ary relation variables X , but no other free variables, if $R \subseteq A^n$ is Σ_1 over $\mathfrak{A}$, then $\theta(R)$ implies $\theta(R')$ for some A -finite $R' \subseteq R$. This may be proved by a straightforward induction

on the way $\theta(X)$ is built up. The key case, when $\theta(X)$ is a restricted universal quantification, requires an application of Σ_1 -collection.

(ii) Let Φ be the set of rules $X \rightarrow \bar{a}$ such that $X \subseteq A^n$ is A -finite and $\bar{a} \in \phi(X)$. Then clearly Φ is a Σ_1 over $\mathfrak{A}$, A -finitary* rule set. Hence by Proposition 3.6.2, $I(\Phi)$ is Σ_1 over $\mathfrak{A}$, so that it suffices to show that $I(\phi) = I(\Phi)$. Note that ϕ is not necessarily the monotone operator associated with Φ , but by (i) it is so on Σ_1 over $\mathfrak{A}$ relations, and this will suffice. To show that $I(\phi) \subseteq I(\Phi)$ it suffices to show that $I(\Phi)$ is ϕ -closed. So let $\bar{x} \in \phi(I(\Phi))$. As $I(\Phi)$ is Σ_1 over $\mathfrak{A}$, by (i) there is an A -finite $X \subseteq I(\Phi)$ such that $\bar{x} \in \phi(X)$. Hence $\Phi : X \rightarrow \bar{x}$ so that $\bar{x} \in I(\Phi)$. To show that $I(\Phi) \subseteq I(\phi)$ it suffices to show that $I(\phi)$ is Φ -closed. So let $\Phi : X \rightarrow \bar{x}$ where $X \subseteq I(\phi)$. Then $\bar{x} \in \phi(X) \subseteq \phi(I(\phi)) = I(\phi)$ as required. Finally, $|\phi| \leq o(A)$ may be seen to follow from the note at the end of the proof of Proposition 3.6.2. $\square$

We end this subsection by stating the central result of BARWISE, GANDY and MOSCHOVAKIS [1971].

3.6.4. DEFINITION. Let A be an admissible set.

(i) $\pi : D \twoheadrightarrow A$ is a *projection of x on A* if $D \subseteq x \in A$ and π is a surjection onto A .

$\mathfrak{A}$ is *projectible to x* if A admits a projection on x that is Δ_1 over $\mathfrak{A}$ (i.e. the graph of the projection and its complement are both Σ_1 over $\mathfrak{A}$).

(ii) $\tau : o(A) \rightarrow A$ is a *resolution of A* if $A = \bigcup_{\alpha < o(A)} \tau(\alpha)$.

$\mathfrak{A}$ is *resolvable* if A admits a resolution that is Δ_1 over $\mathfrak{A}$.

3.6.5. THEOREM (BARWISE, GANDY and MOSCHOVAKIS [1971]). *Let A be any transitive set closed under pairing. Let*

$$A^+ = \bigcap \{B \mid A \in B \text{ and } B \text{ is admissible}\}.$$

Then

(i) A^+ is admissible,

(ii) $\text{HYP}(\mathfrak{A})$ is the set of A^+ -finite relations on A and $\kappa(\mathfrak{A}) = o(A^+)$, and if $\mathfrak{A}^+ = \langle A^+, \in \upharpoonright A^+ \rangle$, then

(iii) $\mathfrak{A}^+$ is resolvable and projectible to A and $\text{IND}(\mathfrak{A})$ is the set of Σ_1 over $\mathfrak{A}^+$ relations on A .

Remarks. The above result has been generalised in two directions. Firstly, $\text{IND}(\mathfrak{A})$ can be replaced by an arbitrary Spector class Γ over $\mathfrak{A} =$

$\langle A, \in \upharpoonright A \rangle$ for any transitive set A . Then A^+ must be replaced by $M(\Delta)$ where $\Delta = \Gamma \cap \neg\Gamma$ and $M(\Delta) = \bigcap \{B \mid \Delta \subseteq B \text{ and } B \text{ is admissible}\}$.

In (ii), $\text{HYP}(\mathfrak{A})$ and $\kappa(\mathfrak{A})$ must be replaced by Δ and $\text{o}(\Gamma)$ respectively. (iii) is replaced by (iii)':

(iii)' There is a relation R on $M(\Delta)$ such that $M(\Delta)$ is admissible relative to R and $\mathcal{M}(\Delta) = \langle M(\Delta), \in \upharpoonright M(\Delta), R \rangle$ is resolvable and projectible to A . Moreover Γ is the set of relations on A that are Σ_1 over $\mathcal{M}(\Delta)$.

Although R and hence $\mathcal{M}(\Delta)$ are not unique the class of relations on $M(\Delta)$ that are Σ_1 over $\mathcal{M}(\Delta)$ is independent of the choice of R and is called the companion of Γ . This generalization is 9E.1. of MOSCHOVAKIS [1974a]. The second generalization is to allow $\mathfrak{A}$ to be an arbitrary abstract structure. This requires the notion of an admissible structure with set A of urelements that has been introduced in BARWISE [1974, 1975]. The details have been worked out in ENNIS [1975]. There, Ennis shows that the result still holds when (ii) in the definition of a Spector class is weakened to (ii)':

(ii)' Γ contains the graph of a pairing function on A .

4. Induction in foundations

In this final section we shall briefly consider the role of inductive definitions in the context of foundations. So far we have taken for granted the standard framework of modern mathematics, formalisable in ZF set theory. But the concept of an inductive definition can also be considered within the other conceptual frameworks that have arisen in work on foundations (e.g. finitist, predicative or intuitionistic mathematics). Within a non-classical framework there arises the question of which inductive definitions can be justified.

It will be helpful to make the distinction between *fundamental* and *non-fundamental* inductive definitions, following the terminology of §53 of KLEENE [1952]. This is a distinction concerning the context in which an inductive definition is presented. The inductive definition of the domain $\mathbf{N}$ of natural numbers is most naturally presented as a fundamental definition of a new sort of object. But in the context of ZF set theory the natural numbers $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots$ are objects that exist independently of the inductive definition of ω . So the latter is a non-fundamental inductive definition. Another example is the inductive definition of the set of even numbers as the smallest set of natural numbers containing 0, and $n + 2$ whenever it contains n .

The standard model of ZF set theory is given by a fundamental inductive definition of the universe of (well-founded) sets. This consists of the collection of rules: If s is a set of objects of the universe, then s itself is an object of the universe.

While the fundamental domains associated with a conceptual framework will usually be explicit, it may require further analysis to decide which non-fundamental inductive definitions are justifiable. For example, given a collection of rules Φ on the domain $\mathbb{N}$ of natural numbers, we have defined $I(\Phi)$ as $\bigcap \{X \subseteq \mathbb{N} \mid X \text{ is } \Phi\text{-closed}\}$, i.e.,

$$n \in I(\Phi) \Leftrightarrow (\forall X \subseteq \mathbb{N})[X \text{ is } \Phi\text{-closed} \rightarrow n \in X].$$

But this is an impredicative instance of the comprehension scheme (a subset of $\mathbb{N}$ is defined using quantification over all subsets of $\mathbb{N}$). If impredicative definitions are not allowed we must look for other possible definitions of $I(\Phi)$. In case Φ is finitary we can use Proposition 1.1.4. In general $I(\Phi)$ could be defined using transfinite iterations of operators, as in Proposition 1.3.1 or transfinite proofs, as in Proposition 1.4.2. But this would require a suitable notion of ordinal which itself would need an inductive definition. An alternative approach is to take induction as a primitive method of definition, not needing justification in terms of other methods.

An example of a formal system treating induction as primitive is the system $\mathbf{ID}_1$ of FEFERMAN [1970] (see also FRIEDMAN [1970], ZUCKER [1973] and MARTIN-LÖF [1971]). The language of $\mathbf{ID}_1$ is obtained from the language of formal arithmetic by adding a new n -ary relation symbol P_ϕ for each arithmetical formula $\phi = \phi(X, \bar{x})$ containing only positive occurrences of the n -ary relation variable X and at most the free individual variables $\bar{x} = x_1, \dots, x_n$. The axioms for $\mathbf{ID}_1$ are obtained from the axioms for formal arithmetic by extending the mathematical induction scheme to all formulae of $\mathbf{ID}_1$ and adding the following axiom and axiom scheme for each P_ϕ .

$$(i) \quad \forall \bar{x} (\phi(P_\phi, \bar{x}) \rightarrow P_\phi(\bar{x})),$$

$$(ii) \quad \forall \bar{x} (\phi(\{\bar{z} \mid \psi(\bar{z})\}, \bar{x}) \rightarrow \psi(\bar{x})) \rightarrow \forall \bar{x} (P_\phi(\bar{x}) \rightarrow \psi(\bar{x})),$$

for all formulae $\psi(\bar{z})$ of $\mathbf{ID}_1$.

In (ii), $\phi(\{\bar{z} \mid \psi(\bar{z})\}, \bar{x})$ denotes the result of replacing each occurrence of $X(\bar{t})$ in $\phi(X, \bar{x})$ by $\psi(\bar{t})$, where $\bar{t} = t_1, \dots, t_n$ is a sequence of terms, and bound variables are changed as required by the usual conventions.

On the standard model of arithmetic these axioms express that P_ϕ is inductively defined by the positive arithmetical operator defined by $\phi(X, \bar{x})$.

The procedure for constructing ID_1 from formal arithmetic may be repeated to obtain $ID_2, ID_3, \dots$. But the resulting systems are still much weaker than fully impredicative systems such as second order arithmetic. On the other hand ID_1 is already stronger than the systems of predicative mathematics of FEFERMAN [1968]. Thus inductive definability is a notion intermediate in strength between predicative and fully impredicative definability.

It would be interesting to formulate a coherent conceptual framework that made induction the principal notion. There are suggestions of this in the literature, but the possibility has not yet been fully explored.

References

AANDERAA, S.

- [1974] Inductive definitions and their closure ordinals, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 207–220.

ACZEL, P.

- [1970] Representability in some systems of second order arithmetic, *Israel J. Math.*, **8**, 309–328.
- [1972] Stage comparison theorem and game playing with inductive definitions, unpublished notes.
- [1973] Infinitary logic and the Barwise compactness theorem, in: *Proceedings of the Bertrand Russell Logic Conference*, edited by J. Bell, J. Cole, G. Priest and A. Slomson (published by the conference) pp. 234–277.
- [1975] Quantifiers, games and inductive definitions, in: *Third Scandinavian Logic Symposium*, edited by S. Kanger (North-Holland, Amsterdam) pp. 1–14.

ACZEL, P. and W. RICHTER

- [1972] Inductive definitions and analogues of large cardinals, in: *Conference in Mathematical Logic — London '70*, Lecture Notes in Mathematics, Vol. 255 (Springer, Berlin) pp. 1–9.

ADDISON, J.W. and S.C. KLEENE

- [1957] A note on function quantification, *Proc. Am. Math. Soc.*, **8**, 1002–1006.

BARWISE, J.

- [1974] Admissible sets over models of set theory, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 97–122.
- [1975] *Admissible Sets and Structures* (Springer, Berlin).

BARWISE, J., R.O. GANDY and Y.N. MOSCHOVAKIS

- [1971] The next admissible set, *J. Symbolic Logic*, **36**, 108–120.

CENZER, D.

- [1974] Ordinal recursion and inductive definitions, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 221–264.

CHANG, C.C. and H.J. KEISLER

- [1973] *Model Theory* (North-Holland, Amsterdam).

ENNIS, G.

- [1975] An extension of the next admissible set construction, mimeographed notes.

FEFERMAN, S.

- [1968] Autonomous transfinite progressions and the extent of predicative mathematics, in: *Logic, Methodology and Philosophy of Science III*, edited by B. van Rootselaar and J.F. Staal (North-Holland, Amsterdam) pp. 121–135.

- [1970] Formal theories for transfinite iterations of generalised inductive definitions and some subsystems of analysis, in: *Intuitionism and Proof Theory*, edited by A. Kino, J. Myhill and R.E. Vesley (North-Holland, Amsterdam) pp. 303–326.

FENSTAD, J.E. and P.G. HINMAN, editors

- [1974] *Generalized Recursion Theory* (North-Holland, Amsterdam).

FRIEDMAN, H.

- [1970] Iterated inductive definitions and Σ_1^1 -AC, in: *Intuitionism and Proof Theory*, edited by A. Kino, J. Myhill and R.E. Vesley (North-Holland, Amsterdam) pp. 435–442.

GANDY, R.O.

- [1974] Inductive definitions, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 265–300.

GRZEGORCZYK, A., A. MOSTOWSKI and C. RYLL-NARDZEWSKI

- [1958] The classical and ω -complete arithmetic, *J. Symbolic Logic*, **23**, 188–206.

GRILLIOT, T.J.

- [1974] Model theory for dissecting recursion theory, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 421–428.

HARRINGTON, L.A.

- [1975] Monotone quantifiers and inductive definability, mimeographed notes.

HARRINGTON, L.A. and A.S. KECHRIS

- [1975] On monotone versus non-monotone induction, mimeographed notes.

KLEENE, S.C.

- [1952] *Introduction to Metamathematics* (Van Nostrand, Princeton, NJ).

KREIDER, D.L. and H. ROGERS

- [1961] Constructive versions of ordinal number classes, *Trans. Am. Math. Soc.*, **100**, 325–369.

MARTIN-LÖF, P.

- [1971] Hauptsatz for the intuitionistic theory of iterated inductive definitions, in: *Proceedings of the Second Scandinavian Logic Symposium*, edited by J.E. Fenstad (North-Holland, Amsterdam) pp. 179–216.

MOSCHOVAKIS, Y.N.

- [1974a] *Elementary Induction on Abstract Structures* (North-Holland, Amsterdam).

- [1974b] On non-monotone inductive definability, *Fund. Math.*, **LXXXII**, 39–83.

- [1976] On the basic notions in the theory of induction, preprint.

PUTNAM, H.

- [1961] Uniqueness ordinals in higher constructive number classes, in: *Essays on the Foundations of Mathematics*, dedicated to A.A. Fraenkel, edited by Y. Bar-Hillel et al. (Magnes Press, Jerusalem) pp. 190–206.

- [1964] On hierarchies and systems of notations, *Proc. Am. Math. Soc.*, **15**, 44–50.

POST, E.

- [1943] Formal reductions of the general combinatorial decision problem, *Am. J. Math.*, **65**, 197–215.

RICHTER, W.

- [1965] Extensions of the constructive ordinals, *J. Symbolic Logic*, **30**, 193–211.

- [1967] Constructive transfinite number classes, *Bull. Am. Math. Soc.*, **73**, 261–265.

- [1968] Constructively accessible ordinal numbers, *J. Symbolic Logic*, **33**, 43–55.
 - [1971] Recursively Mahlo ordinals and inductive definitions, in: *Logic Colloquium '69*, edited by R.O. Gandy and C.E.M. Yates (North-Holland, Amsterdam) pp. 273–288.
 - [1976] The least Σ_2^1 and Π_2^1 reflecting ordinals, to appear.
- RICHTER, W. and P. ACZEL
- [1974] Inductive definitions and reflecting properties of admissible ordinals, in: *Generalized Recursion Theory*, edited by J.E. Fenstad and P.G. Hinman (North-Holland, Amsterdam) pp. 301–384.
- SMULLYAN, R.M.
- [1961] *Theory of Formal Systems* (Princeton University Press, Princeton, NJ).
- SPECTOR, C.
- [1961] Inductively defined sets of natural numbers, in: *Infinistic Methods* (Proceedings of the Warsaw symposium) (Pergamon Press, Oxford) pp. 97–102.
- ZUCKER, J.I.
- [1973] Iterated inductive definitions, trees and ordinals, in: *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*, edited by A.S. Troelstra, Lecture Notes in Mathematics, Vol. 344 (Springer, Berlin).

Descriptive Set Theory: Projective Sets

DONALD A. MARTIN

Contents

Introduction	784
1. Basic concepts of classical descriptive set theory	785
2. Borel and projective sets.	787
3. Structural and regularity properties of pointclasses	795
4. Effective descriptive set theory	799
5. The axiom of constructibility and large cardinal axioms	805
6. Projective determinacy	807
References.	814

Introduction

Our aim is to describe classical and effective descriptive set theory, with emphasis mainly on projective sets. We also give an account of the revival in this subject which has taken place in the last ten years, a revival based on strong set theoretic hypotheses — notably, projective determinacy. Our account has been strongly influenced by writings, lectures, and private remarks of Y.N. Moschovakis and A.S. Kechris.

The study of arbitrary sets of real numbers has been notoriously unsuccessful. Cantor's *continuum hypothesis* asserts that every set of real numbers is countable or has power $2^{\aleph_0}$, the cardinal number of the set of all real numbers. The continuum hypothesis is not merely undecided: the famous theorems of GÖDEL [1940] and COHEN [1963, 1964] show that it is undecidable on the basis of the usual Zermelo–Fraenkel (ZFC) axioms for set theory. Moreover, no candidates for new axioms are available which settle the continuum hypothesis and seem likely to achieve anything like general acceptance. There are other questions about arbitrary sets of real numbers which are less unmanageable, but whose solution leaves a very unsatisfactory situation. The theorem of Vitali asserts that not every set of real numbers is Lebesgue measurable, but its proof depends essentially on the axiom of choice. It remains possible that all sets of real numbers one encounters in practice are Lebesgue measurable.

In descriptive set theory one restricts one's attention to *simple* sets of real numbers: sets of simple topological structure or sets which are definable in some simple way. There are three main advantages to such a restricted interest.

- (1) Many questions which seem unanswerable for arbitrary sets (the continuum hypothesis) can be answered for sufficiently simple sets.
- (2) Many questions which have unpleasant answers for arbitrary sets have pleasant answers for sufficiently simple sets.
- (3) One derives an interesting structural theory of simple sets: a theory of definability.

We can illustrate (1) and (2) by a well-known example. Perhaps the first theorem of descriptive set theory was this: *Every closed set of real numbers is countable or is of power $2^{\aleph_0}$* . Thus no closed set is a counterexample to the continuum hypothesis. This example of (1) is also an example of (2). The full Cantor–Bendixson theorem asserts that *every closed set of real numbers is countable or has a perfect subset* — a closed subset without isolated points. Not all sets of reals have this pleasant property.

Descriptive set theory as we know it today has two independent sources.

First came the classical topological development originated by Borel, Baire, and Lebesgue, and carried out by Souslin, Lusin, Sierpinski, and others. Later, though essentially independently, a different approach to the subject, based on definability and recursive function theory, was produced by Kleene and other logicians. Only in ADDISON [1959a] was it made clear that the two apparently distinct subjects were in fact one subject.

In Sections 1–3 we present the main concepts of the classical theory. In Section 4 we deal with the effective, or Kleene, theory. In Sections 5–6 we discuss questions in descriptive set theory which the ZFC axioms are not sufficient to answer, and we discuss how proposed new axioms for set theory allow one to answer such questions.

1. Basic concepts of classical descriptive set theory

Although in some ways the reals are our main interest, we shall not take the real line as the basic space in terms of which the theory is developed.

One possible reason for this is that the subject applies to many spaces other than the reals. In fact, it applies to any complete separable metric space without isolated points, or *perfect Polish space*. We could then develop the theory for arbitrary perfect Polish spaces. This is, for example, the approach of MOSCHOVAKIS [1978].

We prefer, however, to deal with a single concrete Polish space. We do not use the real line, because that space is slightly awkward to use. Instead we use *Baire space* ω^ω , which we denote by $\mathcal{N}$.

1.1. DEFINITION. ω is the set of all natural numbers. $\mathcal{N}$ is the collection of all functions $\alpha : \omega \rightarrow \omega$. We give ω the discrete topology and, thinking of $\mathcal{N}$ as the product of infinitely many copies of ω , we give $\mathcal{N}$ the product topology.

A base for the non-empty open subsets of $\mathcal{N}$ is the collection of all sets of the form

$$\{\alpha : \bar{\alpha}(n) = \sigma\}$$

where n is a natural number, σ is a sequence of natural numbers of length n , and $\bar{\alpha}(n)$ denotes the finite sequence $\langle \alpha(0), \alpha(1), \dots, \alpha(n-1) \rangle$.

$\mathcal{N}$ is homeomorphic to the space of all irrationals with the topology induced by the inclusion of the irrationals in the reals.

Although we develop the theory for $\mathcal{N}$, most definitions and theorems

apply equally well to any perfect Polish space. (We shall try to note the instances where this fails; but we shall not always indicate the cases when our *proofs* do not work for general spaces.) In fact the theorems for arbitrary perfect Polish spaces usually follow from those for $\mathcal{N}$ using such facts as that any two perfect Polish spaces are “Borel isomorphic”. Some examples of perfect Polish spaces are

(a) the reals,

(b) the Cantor set, which is essentially 2^ω , the set of all $\alpha : \omega \rightarrow \{0, 1\}$, with the topology induced by $2^\omega \subseteq \mathcal{N}$.

$\mathcal{N}$ is homeomorphic to its product with itself. If $\alpha \in \mathcal{N}$, let $\alpha_0(n) = \alpha(2n)$ and $\alpha_1(n) = \alpha(2n + 1)$. The function $f(\alpha) = \langle \alpha_0, \alpha_1 \rangle$ is a homeomorphism. This homeomorphism preserves everything of importance in classical and effective descriptive set theory. Hence the notion of *dimension* plays no role in descriptive set theory. Thus, although our theory deals with finite product spaces $\mathcal{N}^n$, we shall often state definitions and theorems simply for the case $\mathcal{N}$, and no generality is lost in doing so. The fact that the simplest bijection of the reals onto the plane is slightly more complicated than a homeomorphism is one reason we do not base the theory on the reals.

1.2. DEFINITION. Let $\mathcal{Y}$ be the collection of all finite products of $\mathcal{N}$ with itself: $\mathcal{Y} = \{\mathcal{N}, \mathcal{N}^2, \mathcal{N}^3, \dots\}$. Restricting a term of Moschovakis to the present context, we call a subset of an element of $\mathcal{Y}$ a *pointset*.

We are also interested in collections of pointsets. We depart from Moschovakis' terminology by making the irrelevance of dimension part of our definition, even at the cost of a slight artificiality.

1.3. DEFINITION. Let $f : \mathcal{N} \rightarrow \mathcal{N}^2$ be the homeomorphism defined above. If $1 \leq j \leq n$, let $f_j^n : \mathcal{N}^n \rightarrow \mathcal{N}^{n+1}$ be the homeomorphism defined by

$$f_j^n(\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle) = \langle \alpha_1, \alpha_2, \dots, \alpha_{j-1}, (\alpha_j)_0, (\alpha_j)_1, \alpha_{j+1}, \dots, \alpha_n \rangle,$$

where $f(\alpha_j) = \langle (\alpha_j)_0, (\alpha_j)_1 \rangle$. A collection Γ of pointsets is a *pointclass* if, for each n, j , and each $A \subseteq \mathcal{N}^n$,

$$A \in \Gamma \leftrightarrow f_j^n(A) \in \Gamma.$$

A pointclass Γ is then determined completely by $\{A : A \in \Gamma \text{ \& } A \subseteq \mathcal{N}\}$. If we were using the reals instead of $\mathcal{N}$, we could not conveniently make the irrelevance of dimension such a basic part of the theory. Most definitions of particular pointclasses we give later will, nevertheless, make sense for the

reals, and practically all the theorems remain valid for the corresponding “pointclasses” of subsets of finite products of the reals.

1.4. DEFINITION. If $A \subseteq \mathcal{N}^n$ is a pointset, then $\bar{A} = \mathcal{N}^n - A$. If Γ is a pointclass, the *dual* $\check{\Gamma}$ of Γ is defined by

$$A \in \check{\Gamma} \leftrightarrow \bar{A} \in \Gamma.$$

Γ is *self-dual* if $\check{\Gamma} = \Gamma$.

For example, if Γ is the class of all open sets, then $\check{\Gamma}$ is the class of all closed sets. In this case Γ is not self-dual. If Γ is the class of all *clopen* (closed and open) sets, then $\check{\Gamma} = \Gamma$. (The basic open subsets of $\mathcal{N}$ defined above are clopen.)

2. Borel and projective sets

We wish to study the properties of simple or definable subsets of $\mathcal{N}$. This does not mean we study directly the general concept of definable set. There is such a general notion (ordinal definability from reals is the relevant one here), but it is as unmanageable as the notion of arbitrary set of reals. Part of descriptive set theory is indeed general in the sense that one proves that certain properties, typical of definable sets, imply other properties. For the most part, however, we consider only sets which are definable in specific simple ways. In the context of *classical* descriptive set theory, we study the sets derived from the open sets by specific simple operations. The two main kinds of operations we shall consider here are

(a) Boolean algebraic operations
and

(b) projection.

For the moment we consider only (a).

2.1. DEFINITION. A pointset $A \subseteq \mathcal{N}^n$ is *Borel* if A belongs to the σ -algebra generated by the open subsets of $\mathcal{N}^n$.

In other words, the Borel subsets of $\mathcal{N}^n$ are the smallest class Γ containing all open subsets of $\mathcal{N}^n$ and satisfying

$$A \in \Gamma \rightarrow \check{A} \in \Gamma,$$

$$\forall i \in \omega (A_i \in \Gamma) \rightarrow \bigcup_i A_i \in \Gamma.$$

Clearly the class of all Borel subsets of elements of $\mathcal{Y}$ is a pointclass and is self-dual.

We divide the Borel sets into a hierarchy as follows.

2.2. DEFINITION. For countable ordinals $\rho > 0$ we define inductively for fixed $\mathcal{N}^n$:

$$\begin{aligned} A \in \Sigma_1^0 &\leftrightarrow A \text{ is open,} & A \in \Pi_\rho^0 &\leftrightarrow \bar{A} \in \Sigma_\rho^0, \\ A \in \Sigma_\rho^0 &\leftrightarrow \text{there are sets } A_0, A_1, \dots \text{ such that each } A_i \in \Pi_{\rho_i}^0 \\ &\text{for some } \rho_i < \rho \text{ and } A = \bigcup_i A_i \quad (\rho > 1), \\ A \in \Delta_\rho^0 &\leftrightarrow A \in \Sigma_\rho^0 \text{ \& } A \in \Pi_\rho^0. \end{aligned}$$

Each Σ_ρ^0 , Π_ρ^0 , Δ_ρ^0 is a pointclass. It is easy to prove that

$$\bigcup_{0 < \rho < \omega_1} \Sigma_\rho^0 = \text{the class of all Borel sets.}$$

Our notation is that of the Kleene school. Classically sets in Σ_ρ^0 are said to be of *additive class* ρ , sets in Π_ρ^0 of *multiplicative class* ρ , and sets in Δ_ρ^0 of *ambiguous class* ρ . Also $\Sigma_2^0 = \mathbf{F}_\sigma$, $\Pi_2^0 = \mathbf{G}_\delta$, $\Sigma_3^0 = \mathbf{G}_{\delta\sigma}$, etc.

2.3. THEOREM. Σ_ρ^0 , Π_ρ^0 , and Δ_ρ^0 are closed under finite unions, finite intersections, and continuous preimages.

Γ is closed under *continuous preimages* if, whenever $f: \mathcal{N}^n \rightarrow \mathcal{N}^m$ is continuous and $A \in \Gamma$, then $f^{-1}(A) \in \Gamma$. The proof of the theorem is routine.

2.4. DEFINITION. $U \subseteq \mathcal{N}^2$ is *universal* for a pointclass Γ if $U \in \Gamma$ and the set of all sets of the form

$$\{\beta: \langle \alpha, \beta \rangle \in U\}$$

is exactly the collection of subsets of $\mathcal{N}$ which belong to Γ .

Most important non-self-dual pointclasses possess a universal set.

2.5. THEOREM (LEBESGUE [1905]). For each $\rho < \omega_1$ there is a set U universal for Σ_ρ^0 .

PROOF. We first consider the case $\rho = 1$. Let $B_0, B_1, \dots$ be a base for the open subsets of $\mathcal{N}$, with B_0 empty. Let

$$\langle \alpha, \beta \rangle \in U \leftrightarrow \exists n (\beta \in B_{\alpha(n)}).$$

It is easily checked that U is the desired universal set.

Suppose now that $\rho > 1$ and U_ν is universal for Σ_ν^0 for each $\nu < \rho$. Let $g : \omega \rightarrow \{\nu : 1 \leq \nu < \rho\}$ be such that each $g^{-1}(\nu)$ is infinite. Let

$$\langle \alpha, \beta \rangle \in U \leftrightarrow \exists i (\langle \alpha_i, \beta \rangle \notin U_{g(i)}),$$

where $\alpha_i(n) = \alpha(p_i^{n+1})$ with p_i the $(i+1)$ -st prime number. The functions h_i defined by $h_i(\langle \alpha, \beta \rangle) = \langle \alpha_i, \beta \rangle$ are continuous. Since the classes Π_ν^0 are closed under continuous preimages, $\{\langle \alpha, \beta \rangle : \langle \alpha_i, \beta \rangle \notin U_{g(i)}\} \in \Pi_{g(i)}^0$, so $U \in \Sigma_\rho^0$. To prove that U is universal, use the easy fact that $\mathcal{N}^2$ belongs to each Σ_ν^0 . $\square$

2.6. COROLLARY. *For each $\rho < \omega_1$, there is a set U universal for Π_ρ^0 .*

2.7. REMARK. The universal set property is one of a number of properties which tend to hold for $\check{\Gamma}$ if and only if they hold for Γ .

We are now ready to prove a hierarchy theorem for the classes Σ_ρ^0 .

2.8. THEOREM. *Suppose $1 \leq \nu < \rho < \omega_1$. Then $\Delta_\nu^0 \subsetneq \Sigma_\nu^0 \subsetneq \Delta_\rho^0$.*

PROOF. $\Delta_\nu^0 \subseteq \Sigma_\nu^0$ by definition.

The main part of the theorem is $\Sigma_\nu^0 \not\subseteq \Delta_\nu^0$. For this, let U be universal for Σ_ν^0 . Let us put

$$\alpha \in A \leftrightarrow \langle \alpha, \alpha \rangle \in U.$$

$A \in \Sigma_\nu^0$, since Σ_ν^0 is closed under continuous preimages. If $A \in \Delta_\nu^0$, then $A \in \Pi_\nu^0$. This means that for some α

$$\beta \in A \leftrightarrow \langle \alpha, \beta \rangle \notin U.$$

But then

$$\langle \alpha, \alpha \rangle \in U \leftrightarrow \alpha \in A \leftrightarrow \langle \alpha, \alpha \rangle \notin U.$$

$\Sigma_1^0 \subseteq \Sigma_2^0$, since every open set is a countable union of closed sets (the basic open sets). If $1 < \nu \leq \rho$, then by definition $\Sigma_\nu^0 \subseteq \Sigma_\rho^0$. If $1 \leq \nu < \rho$ and $A \in \Pi_\nu^0$, then $A = \bigcup_i A_i$, where each $A_i = A$. Hence $\Pi_\nu^0 \subseteq \Sigma_\rho^0$, and so $\Sigma_\nu^0 \subseteq \Pi_\rho^0$. We then have shown $\Sigma_\nu^0 \subseteq \Delta_\rho^0$ for $1 \leq \nu < \rho$. If $1 \leq \nu < \rho$, then $\Sigma_\nu^0 \neq \Delta_\rho^0$, since $\Sigma_\nu^0 \not\subseteq \Pi_\nu^0 \subseteq \Delta_\rho^0$. $\square$

We now consider a different operation for generating sets from the open sets, the operation of *projection*.

2.9. DEFINITION. If $A \subseteq \mathcal{N}^{n+1}$, the *projection* of A is

$$\{ \langle \alpha_1 \cdots \alpha_n \rangle : \exists \beta \langle \langle \alpha_1, \dots, \alpha_n, \beta \rangle \in A \rangle \}.$$

The projection of A is then a subset of $\mathcal{N}^n$. If we wished to avoid product spaces, we could replace projection in what follows by *continuous image*. The following notion is due to LUSIN [1925] and (apparently independently) SIERPINSKI [1925].

2.10. DEFINITION. The class of *projective sets* is the closure of the open sets under the operations of projection and complementation.

One can show that the projective sets form a pointclass and are closed (within each $\mathcal{N}^n$) under unions and intersections (but not countable unions and intersections). We divide the projective sets into a hierarchy as follows:

2.11. DEFINITION. For $n \in \omega$ we define inductively

$$\Sigma_0^1 = \Sigma_1^0 = \text{the class of open sets,}$$

$$\Pi_n^1 = \check{\Sigma}_n^1,$$

$$A \in \Sigma_{n+1}^1 \leftrightarrow \exists B \in \Pi_n^1 (A \text{ is the projection of } B),$$

$$\Delta_n^1 = \Sigma_n^1 \cap \Pi_n^1.$$

2.12. REMARK. For the reals or 2^ω we must modify the definitions of projective and Σ_n^1 by replacing Σ_1^0 by Σ_2^0 . Classically sets in Σ_1^1 are called *analytic*, sets in Π_1^1 are called CA, sets in Σ_2^1 are called PCA, sets in Π_2^1 are called CPCA, etc.

The Σ_n^1 , Π_n^1 and Δ_n^1 are pointclasses. It is easily proved that the class of projective sets is $\bigcup_n \Sigma_n^1$. Once again we have a universal set theorem and a hierarchy theorem.

2.13. THEOREM. Σ_n^1 , Π_n^1 and Δ_n^1 are closed under finite unions, finite intersections, and continuous preimages.

2.14. THEOREM (Lusin). There is a set U_n universal for Σ_n^1 for each n .

PROOF. Let $U^* \subseteq \mathcal{N}^{n+2}$ be universal for Σ_1^0 . (I.e., the sets of the form $\{ \langle \beta, \beta_1, \dots, \beta_n \rangle : \langle \alpha, \beta, \beta_1, \dots, \beta_n \rangle \in U^* \}$ are exactly the open subsets of $\mathcal{N}^{n+1}$.) Assume n even for definiteness: let

$$\langle \alpha, \beta \rangle \in U_n \leftrightarrow \exists \beta_1 \forall \beta_2 \cdots \forall \beta_n \langle \alpha, \beta, \beta_1, \dots, \beta_n \rangle \in U^*. \quad \square$$

2.15. THEOREM. $\Delta_n^1 \subsetneq \Sigma_n^1 \subsetneq \Delta_{n+1}^1$.

PROOF. The proof is similar to that of Theorem 2.8. $\square$

The Boolean algebraic operations which generate the Borel sets are quite different from the operation of projection. Nevertheless, the two sorts of pointclasses are intimately related. In order to prove a theorem about their relation, we first develop some theory of Π_1^1 which will also be useful later.

Assume n is odd for definiteness. Then $A \subseteq \mathcal{N}$ belongs to Π_n^1 just in case there is an open set $B \subseteq \mathcal{N}^{n+1}$ such that

$$\alpha \in A \leftrightarrow \forall \beta_1 \exists \beta_2 \cdots \forall \beta_n \langle \alpha, \beta_1, \dots, \beta_n \rangle \in B.$$

The theorem below follows by the definition of open set.

2.16. THEOREM. $A \in \Pi_n^1$, n odd [$A \in \Sigma_n^1$, n even], just in case there is a relation R such that

$$\begin{aligned} \alpha \in A &\leftrightarrow \forall \beta_1 \exists \beta_2 \cdots \forall \beta_n \exists m R(\bar{\alpha}(m), \bar{\beta}_1(m), \dots, \bar{\beta}_n(m)), \\ &[\alpha \in A \leftrightarrow \exists \beta_1 \forall \beta_2 \cdots \forall \beta_n \exists m R(\bar{\alpha}(m), \bar{\beta}_1(m), \dots, \bar{\beta}_n(m))], \end{aligned}$$

where $\bar{\beta}(m)$ denotes the sequence $\langle \beta(0), \dots, \beta(m-1) \rangle$.

If $A \in \Pi_1^1$, there is an R such that

$$\alpha \in A \leftrightarrow \forall \beta \exists m R(\bar{\alpha}(m), \bar{\beta}(m)).$$

For such an R , define for $\alpha \in \mathcal{N}$,

$$X_{\alpha, R} = \{ \bar{\beta}(m) : \forall n \leq m \neg R(\bar{\alpha}(n), \bar{\beta}(n)) \}.$$

Let Seq be the collection of all finite sequences of natural numbers.

2.17. DEFINITION. If $\sigma, \tau \in \text{Seq}$, let $\sigma < \tau$ mean that σ is a proper extension of τ . $<$ is a partial ordering of Seq.

2.18. THEOREM. For A, R as above,

$$\alpha \in A \leftrightarrow < \text{ is well-founded on } X_{\alpha, R}.$$

PROOF. Infinite descending chains in $X_{\alpha, R}$ correspond to functions β such that $\forall m \neg R(\bar{\alpha}(m), \bar{\beta}(m))$. $\square$

2.19. DEFINITION. Let $<$ be a well-founded relation on a set X . For $x \in X$, define $|x|<$ inductively by

$$|x|< = \sup_{y < x} (|y|< + 1).$$

The *length* of $<$ is

$$\sup_{x \in X} (|x|< + 1).$$

We are now ready to state and prove one of the most important theorems of descriptive set theory.

2.20. SOUSLIN THEOREM. $\Delta_1^1 =$ the class of all Borel sets.

PROOF. The open sets belong to Δ_1^1 by Theorem 2.15, since $\Sigma_1^0 = \Sigma_0^1 \subseteq \Delta_1^1$. We prove that Δ_1^1 is closed under countable unions and complements. The case of complements is immediate.

Let $A = \bigcup_i A_i$ with each $A_i \in \Delta_1^1$. Since each $A_i \in \Sigma_1^1$,

$$\alpha \in A_i \leftrightarrow \exists \beta \langle \alpha, \beta \rangle \in B_i$$

with B_i closed. Hence

$$\alpha \in A \leftrightarrow \exists i \exists \beta \langle \alpha, \beta \rangle \in B_i \leftrightarrow \exists \beta \langle \alpha, \beta' \rangle \in B_{\beta(0)}$$

where $\beta'(n) = \beta(n+1)$. $\{\langle \alpha, \beta \rangle : \langle \alpha, \beta' \rangle \in B_{\beta(0)}\}$ is closed. Since each $A_i \in \Pi_1^1$,

$$\alpha \in A_i \leftrightarrow \forall \beta \langle \alpha, \beta \rangle \in B_i$$

with each B_i open. But then

$$\alpha \in A \leftrightarrow \exists i \forall \beta \langle \alpha, \beta \rangle \in B_i \leftrightarrow \forall \beta \exists i \langle \alpha, \beta_i \rangle \in B_i$$

where $\beta_i(n) = \beta(p_i^{n+1})$ with p_i the $(i+1)$ -st prime number. Clearly the second implies the third; and if $\forall i \exists \beta (i) \langle \alpha, \beta(i) \rangle \notin B_i$, let $\beta_i = \beta(i)$ and we have $\forall i \langle \alpha, \beta_i \rangle \notin B_i$. Since

$$\{\langle \alpha, \beta \rangle : \exists i \langle \alpha, \beta_i \rangle \in B_i\}$$

is open, we have shown that $A \in \Sigma_1^1 \cap \Pi_1^1 = \Delta_1^1$. $\square$

Now consider any $A \in \Pi_1^1$. Let R be as guaranteed by Theorem 2.16. By Theorem 2.18,

$$\alpha \in A \leftrightarrow < \text{ is well-founded on } X_{\alpha, R}.$$

2.21. LEMMA. Suppose $\exists \rho < \omega_1 \forall \alpha \in A$ ($< \upharpoonright X_{\alpha, R}$ has length $\leq \rho$). Then A is Borel.

PROOF. For $\sigma \in X_{\alpha, R}$, let $|\sigma|_\alpha = |\sigma|^{< \upharpoonright X_{\alpha, R}}$. We show by induction on $\rho < \omega_1$ that, for each $\sigma \in \text{Seq}$

$$\{\alpha : \sigma \notin X_{\alpha, R} \text{ or } |\sigma|_\alpha \leq \rho\}$$

is Borel. For $\rho = 0$,

$$\{\alpha : \sigma \notin X_{\alpha, R} \text{ or } |\sigma|_\alpha = 0\} = \bigcap_{\tau < \sigma} \{\alpha : \tau \notin X_{\alpha, R}\},$$

which is closed, since $\{\alpha : \tau \in X_{\alpha, R}\}$ is clopen for each τ .

If $\rho > 0$,

$$\{\alpha : \alpha \notin X_{\alpha, R} \text{ or } |\sigma|_\alpha \leq \rho\} = \bigcap_{\tau < \sigma} \bigcup_{\nu < \rho} \{\alpha : \tau \notin X_{\alpha, R} \text{ or } |\tau|_\alpha \leq \nu\}.$$

The lemma follows, since under its hypotheses,

$$\begin{aligned} A &= \{\alpha : < \upharpoonright X_{\alpha, R} \text{ is well-founded with length } \leq \rho\} \\ &= \bigcap_{\sigma \in \text{Seq}} \bigcup_{\nu < \rho} \{\alpha : \sigma \notin X_{\alpha, R} \text{ or } |\sigma|_\alpha \leq \nu\}. \quad \square \end{aligned}$$

Suppose now that $A \in \Delta_1^1$. Let R and S satisfy

$$\alpha \in A \leftrightarrow \forall \beta \exists n R(\bar{\alpha}(n), \bar{\beta}(n));$$

$$\alpha \in \bar{A} \leftrightarrow \forall \gamma \exists n S(\bar{\alpha}(n), \bar{\gamma}(n)).$$

Let Y be the set of all triples $\langle \bar{\alpha}(n), \bar{\beta}(n), \bar{\gamma}(n) \rangle$ such that

$$\bar{\beta}(n) \in X_{\alpha, R} \text{ \& \> } \bar{\gamma}(n) \in X_{\alpha, S}.$$

(Note that this condition depends only on the finite sequence $\bar{\alpha}(n)$.) Say that

$$\langle \bar{\alpha}_1(n), \bar{\beta}_1(n), \bar{\gamma}_1(n) \rangle < \langle \bar{\alpha}_2(n), \bar{\beta}_2(n), \bar{\gamma}_2(n) \rangle \leftrightarrow$$

$$\bar{\alpha}_1(n) < \bar{\alpha}_2(n) \text{ \& \> } \bar{\beta}_1(n) < \bar{\beta}_2(n) \text{ \& \> } \bar{\gamma}_1(n) < \bar{\gamma}_2(n).$$

$<$ is well-founded on Y , since an infinite descending chain in Y would give a triple $\langle \alpha, \beta, \gamma \rangle$ such that

$$\forall n \neg R(\bar{\alpha}(n), \bar{\beta}(n)) \text{ \& \> } \forall n \neg S(\bar{\alpha}(n), \bar{\gamma}(n))$$

and so $\alpha \notin A \cup \bar{A}$.

Let ρ be the length of $< \upharpoonright Y$. Suppose $\alpha \in A$. Let γ satisfy $\forall n \neg S(\bar{\alpha}(n), \bar{\gamma}(n))$. Define

$$\phi(\bar{\beta}(n)) = \langle \bar{\alpha}(n), \bar{\beta}(n), \bar{\gamma}(n) \rangle;$$

ϕ maps $X_{\alpha, R}$ into Y in a one-one order-preserving manner. Hence the length of $<\restriction X_{\alpha, R}$ is $\leq \rho$, and so A is Borel by the Lemma. $\square$

2.22. COROLLARY (to the first half of the proof, easily generalized). Σ_n^1 and Π_n^1 are closed under countable unions and intersections for $n \geq 1$.

There are further relations between the projective hierarchy and the sets gotten by closing the open sets under Boolean algebraic operations. For these we need to consider uncountable unions and intersections.

2.23. THEOREM (SIERPINSKI [1925]). Every $A \in \Sigma_2^1$ is a union of $\aleph_1$ Borel sets.

PROOF (outline). We sketch the proof. The proof of the Souslin Theorem already shows that every $A \in \Pi_1^1$ is a union of $\aleph_1$ Borel sets:

$$A = \bigcup_{\rho < \omega_1} \{\alpha: <\restriction X_{\alpha, R} \text{ is well-founded with length } \leq \rho\}.$$

2.24. LEMMA. Every $A \in \Sigma_1^1$ is a union of $\aleph_1$ Borel sets.

PROOF. Let $A = \{\alpha: \exists \beta \forall n R(\bar{\alpha}(n), \bar{\beta}(n))\}$. Let us order $\mathcal{N}$ by $\beta_1 \triangleleft \beta_2 \leftrightarrow \beta_1 \neq \beta_2$ and the least n with $\beta_1(n) \neq \beta_2(n)$ satisfies $\beta_1(n) < \beta_2(n)$. It is easily checked that, for $\alpha \in A$ there is a least $\beta = \beta(\alpha)$ such that $\forall n R(\bar{\alpha}(n), \bar{\beta}(n))$. For $\alpha \in A$ define

$$Z_\alpha = \{\bar{\gamma}(n): \gamma \triangleleft \beta(\alpha) \ \& \ \bar{\gamma}(n) \neq \overline{\beta(\alpha)}(n) \ \& \ \forall m \leq n R(\bar{\alpha}(m), \bar{\gamma}(m))\}.$$

Clearly $<$ is well-founded on Z_α . Now define, for $\rho < \omega_1$,

$$A_\rho = \{\alpha: \alpha \in A \ \& \ <\restriction Z_\alpha \text{ has length } \leq \rho\}.$$

Clearly $A = \bigcup_{\rho < \omega_1} A_\rho$. An argument similar to that in the proof of the Souslin Theorem shows that each A_ρ is Borel. $\square$

Now let $A \in \Sigma_2^1$. By Theorem 2.16 there is a relation R such that

$$\alpha \in A \leftrightarrow \exists \beta \forall \gamma \exists n R(\bar{\alpha}(n), \bar{\beta}(n), \bar{\gamma}(n)).$$

But then,

$$\alpha \in A \leftrightarrow \exists \beta (<\restriction X_{\alpha, \beta, R} \text{ is well-founded}),$$

where $X_{\alpha, \beta, R}$ has the obvious meaning. Then

$$\alpha \in A \leftrightarrow \exists \beta \exists \rho < \omega_1 (<\restriction X_{\alpha, \beta, R} \text{ is well-founded with length } \leq \rho)$$

$$\leftrightarrow \exists \rho < \omega_1 \exists \beta (<\restriction X_{\alpha, \beta, R} \text{ is well-founded with length } \leq \rho)$$

$$\leftrightarrow \exists \rho < \omega_1 \exists \beta \exists f: X_{\alpha, \beta, R} \rightarrow \rho \ (f \text{ is order preserving}).$$

By coding β and f into a single function $\gamma : \omega \rightarrow \omega$, we see that

$$\{\alpha : \exists \beta \exists f : X_{\alpha, \beta, R} \rightarrow \rho \text{ (} f \text{ is order-preserving)}\} \in \Sigma_1^1$$

for each ρ . Hence A is the union of $\aleph_1$ elements of Σ_1^1 . The Lemma implies the Theorem. $\square$

It is known that one cannot prove or refute from the ZFC axioms the converse of Theorem 2.23: that every union of $\aleph_1$ Borel sets belongs to Σ_2^1 .

3. Structural and regularity properties of pointclasses

The structural properties of Σ_n^1 and Σ_p^0 we have derived so far are also properties of Π_n^1 and Π_p^0 . (Theorem 2.23 is an exception.) But there are other, deeper structural properties for which this is not the case. (There are also some shallow properties for which it is not the case. For instance, Σ_n^0 but not Π_n^0 is closed under countable unions.) One of the fundamental empirical principles of descriptive set theory is the following:

There is a collection $\mathcal{P}$ of interesting structural properties such that, if Γ is an important non-self-dual pointclass, then either Γ or $\check{\Gamma}$ but never both has most or all of the properties in $\mathcal{P}$.

The proof that Γ and $\check{\Gamma}$ cannot both have a property in $\mathcal{P}$ is usually easy and depends only on general principles. The difficulty lies in showing that one of the classes has the property in question. Sometimes this difficulty amounts to impossibility if one is limited to the ZFC axioms.

3.1. DEFINITION. *Reduction(Γ)* means that, for all $A, B \in \Gamma$ with $A, B \subseteq \mathcal{N}^n$, there are $A', B' \in \Gamma$ such that

$$A' \subseteq A, \quad B' \subseteq B, \quad A' \cup B' = A \cup B,$$

and $A' \cap B'$ is empty (see Fig. 1).

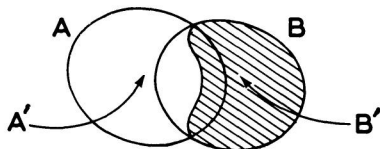


Fig. 1.

Reduction can never hold for both Γ and $\check{\Gamma}$ if Γ has certain basic properties

3.2. THEOREM. *If Γ is a pointclass with a universal set and closed under continuous preimages, then Reduction fails for Γ or $\check{\Gamma}$.*

PROOF. Let U be universal for Γ and let $\alpha \rightarrow \langle \alpha_0, \alpha_1 \rangle$ be the canonical homeomorphism of $\mathcal{N}$ onto $\mathcal{N}^2$. Let

$$A = \{\langle \alpha, \beta \rangle : \langle \alpha_0, \beta \rangle \in U\}; \quad B = \{\langle \alpha, \beta \rangle : \langle \alpha_1, \beta \rangle \in U\}.$$

If $\text{Reduction}(\Gamma)$, let A', B' be as given by $\text{Reduction}(\Gamma)$. If $\text{Reduction}(\check{\Gamma})$, let A^*, B^* be as given by applying $\text{Reduction}(\check{\Gamma})$ to $\overline{A'}, \overline{B'}$. $A^* = \overline{B^*}$, so $A^* \in \Gamma \cap \check{\Gamma}$. If $\{\beta : \langle \alpha_0, \beta \rangle \in U\}$ is the complement of $\{\beta : \langle \alpha_1, \beta \rangle \in U\}$ then $\langle \alpha, \beta \rangle \in \overline{A^*} \leftrightarrow \langle \alpha, \beta \rangle \in A$ and $\langle \alpha, \beta \rangle \in \overline{B^*} \leftrightarrow \langle \alpha, \beta \rangle \in B$. Hence every $C \in \Gamma \cap \check{\Gamma}$ is of the form $\{\beta : \langle \alpha, \beta \rangle \in A^*\}$.

Now let

$$\alpha \in C \leftrightarrow \langle \alpha, \alpha \rangle \in A^*.$$

Since Γ is closed under continuous preimages, $C \in \Gamma \cap \check{\Gamma}$. But then for some α , $C = \{\beta : \langle \alpha, \beta \rangle \notin A^*\}$. Thus

$$\langle \alpha, \alpha \rangle \in A^* \leftrightarrow \alpha \in C \leftrightarrow \langle \alpha, \alpha \rangle \notin A^*. \quad \square$$

A stronger property than Reduction is the following:

3.3. DEFINITION. *Prewellordering* (Γ) means that for every $A \in \Gamma$ there is a function $\phi : A \rightarrow \text{Ordinals}$ and there are R, S in $\check{\Gamma}$ such that, for $\beta \in A$,

$$\alpha \in A \ \& \ \phi(\alpha) < \phi(\beta) \leftrightarrow \langle \alpha, \beta \rangle \in R;$$

$$\alpha \in A \ \& \ \phi(\alpha) \leq \phi(\beta) \leftrightarrow \langle \alpha, \beta \rangle \in S.$$

3.4. THEOREM. *Prewellordering* (Γ) $\rightarrow$ *Reduction* (Γ), provided that Γ is closed under finite unions, finite intersections, and continuous preimages.

PROOF. Let $A, B \in \Gamma$. Let

$$C_1 = \{\langle \alpha, \beta \rangle : \alpha(0) = 0 \ \& \ \beta \in A\}; \quad C_2 = \{\langle \alpha, \beta \rangle : \alpha(0) = 1 \ \& \ \beta \in B\}.$$

Let $C = C_1 \cup C_2$. By the closure properties, $C \in \Gamma$. Let $\phi : C \rightarrow \text{Ordinals}$ be as given by Prewellordering (Γ). Set

$$A' = A \cap \{\beta : \langle 1, \beta \rangle \notin C \text{ or } \phi\langle 0, \beta \rangle < \phi\langle 1, \beta \rangle\};$$

$$B' = B \cap \{\beta : \langle 0, \beta \rangle \notin C \text{ or } \phi\langle 1, \beta \rangle \leq \phi\langle 0, \beta \rangle\},$$

where 0 and 1 are respectively the functions which are identically 0 and 1. By the properties of ϕ and the closure properties, A' and B' belong to Γ . It

is easy to check that A' and B' have the properties required by Reduction. $\square$

Reduction is only one of a large collection of structural properties which follow from Prewellordering.

3.5. THEOREM. *For all ρ , $1 \leq \rho < \omega_1$, Prewellordering (Σ_ρ^0).*

PROOF. Let $A \in \Sigma_\rho^0$. Then $A = \bigcup_i A_i$ with each $A_i \in \Delta_\rho^0$. We may assume that $i < j$ implies $A_i \subseteq A_j$. Define, for each $\alpha \in A$

$$\phi(\alpha) = \text{the least } i \text{ such that } \alpha \in A_i.$$

If $\beta \in A$, then

$$\alpha \in A \ \& \ \phi(\alpha) < \phi(\beta) \leftrightarrow (\beta \notin A_0 \ \& \ \forall i (\beta \in A_{i+1} \rightarrow \alpha \in A_i));$$

$$\alpha \in A \ \& \ \phi(\alpha) \leq \phi(\beta) \leftrightarrow \forall i (\beta \in A_i \rightarrow \alpha \in A_i).$$

The relations on the right belong to Π_ρ^0 . $\square$

3.6. REMARK. For Σ_1^0 , the theorem fails for the reals.

3.7. THEOREM. *Prewellordering (Π_1^1).*

PROOF. Let R witness that $A \in \Pi_1^1$,

$$\alpha \in A \leftrightarrow < \upharpoonright X_{\alpha, R} \text{ is well-founded.}$$

Let $\phi(\alpha)$ be the length of $< \upharpoonright X_{\alpha, R}$. If $\beta \in A$, then

$$\alpha \in A \ \& \ \phi(\alpha) < \phi(\beta) \leftrightarrow$$

$$\leftrightarrow \exists f [f: X_{\alpha, R} \rightarrow X_{\beta, R} \ \& \ (\sigma < \tau \rightarrow f(\sigma) < f(\tau))]$$

& the empty sequence is not in the range of f],

$$\alpha \in A \ \& \ \phi(\alpha) \leq \phi(\beta) \leftrightarrow \exists f [f: X_{\alpha, R} \rightarrow X_{\beta, R} \ \& \ (\sigma < \tau \rightarrow f(\sigma) < f(\tau))].$$

To prove this, let $\phi(\alpha) \leq \phi(\beta)$, and define $f(\sigma)$ by induction on the length of σ so that $|f(\sigma)|_\beta = |\sigma|_\alpha$. f can be construed as a function from ω to ω , so both relations on the right belong to Σ_1^1 . $\square$

3.8. THEOREM (Moschovakis). *Prewellordering (Π_n^1) $\rightarrow$ Prewellordering (Σ_{n+1}^1)*

PROOF. Let $A \in \Sigma_{n+1}^1$. For some $B \in \Pi_n^1$, $\alpha \in A \leftrightarrow (\exists \beta) \langle \alpha, \beta \rangle \in B$. Let $\phi : B \rightarrow \text{Ordinals}$ be as demanded by $\text{Prewellordering}(\Pi_n^1)$. For $\alpha \in A$ set

$$\psi(\alpha) = \inf\{\phi\langle \alpha, \gamma \rangle : \langle \alpha, \gamma \rangle \in B\}.$$

A routine computation shows that the required relations R and S exist. $\square$

3.9. COROLLARY. *Prewellordering* (Σ_2^1) .

3.10. REMARK. The abstract notion of *Prewellordering* was probably first isolated by Moschovakis, though in some sense $\text{Prewellordering}(\Pi_1^1)$ is a classical result. $\text{Reduction}(\Pi_1^1)$ is a theorem of Kuratowski.

Some of the structural properties of Π_1^1 and Σ_2^1 are not implied by *Prewellordering*. The best-known such property is *Uniformization*. We postpone the subject of *Uniformization* until Section 4, where its significance can be made more clear in terms of the effective theory.

We consider the following three regularity properties.

3.11. DEFINITION. (i) A has the *Baire property* if A differs from an open set by a set of the first category. A set is of the *first category* if it is disjoint from a countable intersection of dense open sets.

(ii) A has the *perfect subset property* if A is countable or has a perfect subset.

(iii) Definitions (i) and (ii) make sense in general spaces. For $A \subseteq \text{Reals}$, A is *measurable* if A is Lebesgue measurable. For $A \subseteq \mathcal{N}$, we say A is *measurable* if A is measurable when construed as a set of irrationals. For $A \subseteq 2^\omega$, A is *measurable* if A is measurable with respect to the product of the measure on $\{0, 1\}$ gotten by giving $\{0\}$ and $\{1\}$ measure $\frac{1}{2}$.

There exist sets not satisfying any of (i), (ii) or (iii). However:

3.12. THEOREM. $A \in \Sigma_1^1 \rightarrow A$ is measurable (LUSIN [1917]), has the *Baire property* (LUSIN and SIERPINSKI [1923]), and has the *perfect subset property* (Souslin).

3.13. COROLLARY. $A \in \Pi_1^1 \rightarrow A$ is measurable and has the *Baire property*.

PROOF. These properties hold of A if and only if they hold of $\bar{A}$. $\square$

3.14. COROLLARY. $A \in \Sigma_1^1 \rightarrow A$ is countable or of power $2^{\aleph_0}$.

3.15. COROLLARY. $A \in \Sigma_2^1 \rightarrow A$ is countable, has power $\aleph_1$, or has power $2^{\aleph_0}$.

PROOF. Apply Theorem 2.23. $\square$

4. Effective descriptive set theory

The advent of effective descriptive set theory brought two main improvements to the classical theory.

(1) The effective theory extends and refines the classical theory to give a genuine theory of *definability*, including a theory for reals as well as sets of reals.

(2) The founders (principally Kleene) of the effective theory introduced superior notation (which we have been using) and a variety of results and techniques, including coding techniques, which greatly facilitate proofs even of assertions of the classical theory.

Recall that a subset A of $\mathcal{N}^n$ belongs to Σ_k^1 for k odd just in case there is a relation R such that

$$\langle \alpha_1, \dots, \alpha_n \rangle \in A \leftrightarrow$$

$$(*) \quad \leftrightarrow \exists \beta_1 \forall \beta_2 \cdots \exists \beta_k \forall m R(\bar{\alpha}_1(m), \dots, \bar{\alpha}_n(m), \bar{\beta}_1(m), \dots, \bar{\beta}_k(m)).$$

For k even there is a similar representation, with $\forall \beta_k \exists m$ replacing $\exists \beta_k \forall m$.

4.1. DEFINITION. $A \subseteq \mathcal{N}^n$ belongs to Σ_k^1 for k odd just in case there is a *recursive* relation R such that $(*)$ holds, where the notion of recursive relations among finite sequences is defined in the natural way from that of recursive relations on the natural numbers. The definition of Σ_k^1 for k even is similar.

4.2. DEFINITION. If $\alpha \in \mathcal{N}$, $A \subseteq \mathcal{N}^n$, k odd, then $A \in \Sigma_k^1(\alpha)$ just in case there is an R recursive in α such that $(*)$ holds; similarly for k even.

These effective concepts contain the classical concepts since

$$\Sigma_n^1 = \bigcup_{\alpha \in \mathcal{N}} \Sigma_n^1(\alpha).$$

4.3. DEFINITION. $\Pi_n^1 = \check{\Sigma}_n^1$. $\Delta_n^1 = \Sigma_n^1 \cap \Pi_n^1$. Similarly for $\Pi_n^1(\alpha)$ and $\Delta_n^1(\alpha)$.

The effective projective hierarchy makes sense also for subsets of ω as well as subsets of $\mathcal{N}$.

4.4. DEFINITION. Assume k odd for definiteness. If $A \subseteq \omega^{n_1} \times \mathcal{N}^{n_2}$, then $A \in \Sigma_k^1$ just in case there is a recursive relation R such that

$$\langle a_1, \dots, a_{n_1}, \alpha_1, \dots, \alpha_{n_2} \rangle \in A \leftrightarrow$$

$$\leftrightarrow \exists \beta_1 \forall \beta_2 \cdots \exists \beta_k \forall m R(a_1, \dots, a_{n_1}, \bar{\alpha}_1(m), \dots, \bar{\alpha}_{n_2}(m), \bar{\beta}(m), \dots, \bar{\beta}_k(m)).$$

Other notions are defined similarly. The notion of a *pointset* is extended to include subsets of $\omega^{n_1} \times \mathcal{N}^{n_2}$ and the notion of a *pointclass* is extended so that a pointclass is a collection of pointsets closed under our canonical homeomorphisms and also under canonical recursive bijections $\omega^n \rightarrow \omega^m$.

A refinement of the finite Borel hierarchy can also be defined for the effective theory. It is easily seen that a set $A \subseteq \mathcal{N}^n$ belongs to Σ_k^0 , for odd k , just in case there is a relation R such that

$$(**) \quad \alpha \in A \leftrightarrow \exists a_1 \forall a_2 \cdots \exists a_k R(\bar{\alpha}(a_k), a_1, \dots, a_{k-1}).$$

where the a_k range over natural numbers.

4.5. DEFINITION. $\Sigma_n^0, \Pi_n^0, \Delta_n^0, \Sigma_n^0(\alpha), \Pi_n^0(\alpha), \Delta_n^0(\alpha)$ are defined using (**) in the same way the effective projective pointclasses were defined using (*). Elements of Σ_1^0 are called *semirecursive* or *recursively enumerable*; elements of Δ_1^0 are called *recursive*.

With slight modifications, the effective notions can be defined for other Polish spaces such as 2^ω and the reals. As with the classical theory the class Σ_1^0 tends to behave differently for spaces other than $\mathcal{N}$, and some of the results which follow are valid for that class only in $\mathcal{N}$.

The notion of Borel set also has an effective refinement, the notion of a *hyperarithmetical* set. We omit the definition, and content ourselves with remarking that ω_1 is replaced by *Church–Kleene* ω_1 , the least ordinal not the order type of a recursive wellordering of a subset of ω .

4.6. DEFINITION. If $\alpha \in \mathcal{N}^n$ and Γ is a pointclass, $\alpha \in \Gamma$ just in case

$$\{\langle a_1, a_2 \rangle : \alpha(a_1) = a_2\} \in \Gamma.$$

In other words, a function belongs to Γ if and only if its *graph* belongs to Γ .

All the theorems of classical descriptive set theory have effective refinements. We state the following results for the Σ_k^0 and Σ_k^1 , but the relativizations to $\Sigma_k^0(\alpha)$ and $\Sigma_k^1(\alpha)$ also hold and imply the corresponding classical results. The proofs of the classical theorems are sufficiently effective to yield proofs of the effective theorems. Many of the theorems which follow are due to Kleene. (See KLEENE [1952] and [1955].)

We first describe the effective analogue of a continuous function. In Section 1 we gave a base for the non-empty open subsets of $\mathcal{N}$. We give ω the discrete topology and take as a base for its non-empty open subsets the collection of all singletons. A basic open subset of $\omega^{m_1} \times \mathcal{N}^{m_2}$ is a product of basic open subsets of the factors. Let $B_0, B_1, \dots$ be an effective enumeration of the basic open subsets of $\omega^{m_1} \times \mathcal{N}^{m_2}$ (i.e. an effective enumeration of the finite sequences of natural numbers which determine the basic open sets).

4.7. DEFINITION. $F: \omega^{n_1} \times \mathcal{N}^{n_2} \rightarrow \omega^{m_1} \times \mathcal{N}^{m_2}$ is *recursive* if

$$\{\langle k, a_1, \dots, a_{n_1}, \alpha_1, \dots, \alpha_{n_2} \rangle: f(\langle a_1, \dots, a_{n_1}, \alpha_1, \dots, \alpha_{n_2} \rangle) \in B_k\} \in \Delta_1^0.$$

4.8. THEOREM. If $\Gamma = \Sigma_n^0, \Pi_n^0, \Delta_n^0, \Sigma_n^1, \Pi_n^1$, or Δ_n^1 , then Γ is closed under finite unions, finite intersections and recursive preimages.

4.9. THEOREM. Let Γ be $\Sigma_n^0, \Pi_n^0, \Sigma_n^1$, or Π_n^1 and let Γ be the corresponding $\Sigma_n^0, \Pi_n^0, \Sigma_n^1$, or Π_n^1 .

There is a $U \in \Gamma$ which is universal for Γ ; there is a $U \subseteq \omega \times \mathcal{N}$ with $U \in \Gamma$ such that the sets of the form

$$\{\beta: \langle b, \beta \rangle \in U\}$$

are exactly the subsets of $\mathcal{N}$ which belong to Γ .

PROOF. For the proof of the second half of the theorem, one uses the enumeration theorem of recursion theory to handle the case $\Gamma = \Sigma_1^0$. $\square$

4.10. THEOREM. $\Delta_n^0 \subsetneq \Sigma_n^0 \subsetneq \Delta_{n+1}^0$; $\Delta_n^1 \subsetneq \Sigma_n^1 \subsetneq \Delta_{n+1}^1$.

The extension of the first part of Theorem 4.10 to transfinite levels, which we have not defined, also holds.

The effective analogue of Theorem 2.20 is due to Kleene and asserts

$$\text{The class of hyperarithmetical sets} = \Delta_1^1.$$

4.11. THEOREM. *Prewellordering* (Σ_n^0) . *Prewellordering* (Π_1^1) *Prewellordering* $(\Pi_n^1) \rightarrow \text{Prewellordering}(\Sigma_{n+1}^1)$.

4.12. COROLLARY. *Prewellordering* (Σ_2^1) .

The effective concepts are defined in terms of recursive function theory, but there are other, equivalent definitions. The *language of arithmetic* is the language in first order logic with function symbols for addition, multiplication and successor and a symbol for 0.

4.13. DEFINITION. A set A of natural numbers is *arithmetical* if there is a formula $\phi(x)$ of the language of arithmetic with only the variable x free such that

$$n \in A \leftrightarrow N \models \phi[n]$$

where N is the standard model of arithmetic.

4.14. THEOREM. A is *arithmetical* $\leftrightarrow A \in \bigcup_n \Sigma_n^0$.

Hence $\bigcup_n \Sigma_n^0$ consists just of those sets definable in arithmetic. The definition of arithmetical can be extended to subsets of $\omega^m \times \mathcal{N}^n$ and Theorem 4.14 remains true.

The *language of analysis* is gotten from the language of arithmetic by introducing variables to range over functions from ω to ω and quantifying also over such variables.

4.15. DEFINITION. $A \subseteq \omega^m \times \mathcal{N}^n$ is *analytical* if there is a formula ϕ of analysis such that

$$\langle a_1 \cdots a_m, \alpha_1 \cdots \alpha_n \rangle \in A \leftrightarrow M \models \phi[a_1 \cdots a_m, \alpha_1 \cdots \alpha_n]$$

where M is the standard model of analysis.

4.16. THEOREM. A is *analytical* $\leftrightarrow A \in \bigcup_n \Sigma_n^1$.

The theorem asserts that $\bigcup_n \Sigma_n^1$ consists of just those sets definable in analysis.

The effective theory allows one to raise a new kind of question: *if a simply definable subset of $\mathcal{N}$ has a member, does it have a simply definable member?* To make this question more precise, we give a definition.

4.17. DEFINITION. Γ_1 is a *basis* for Γ_2 if for every non-empty $A \in \Gamma_2$, $A \subseteq \mathcal{N}$, there is an element of $A \cap \Gamma_1$.

Here are a positive basis result and a negative basis result.

4.18. THEOREM (Kleene). Δ_1^0 is a basis for Σ_1^0 . Δ_1^1 is not a basis for Π_1^0 .

PROOF. The first part of the theorem follows from the fact that $A \in \Sigma_1^0 \rightarrow A$ has an eventually constant member. For the second part let $A \subseteq \mathcal{N}$, $A = \Delta_1^1 \cap \mathcal{N}$. It can be shown that $A \in \Pi_1^1$. Let $\alpha \notin A \leftrightarrow \exists \beta (\langle \alpha, \beta \rangle \in B)$ with $B \in \Pi_0^1 = \Pi_1^0$. If $\langle \alpha, \beta \rangle \in B \cap \Delta_1^1$, then $\alpha \in \Delta_1^1$, a contradiction. $\square$

Often basis theorems can be improved by strengthening them to *uniformization* theorems.

4.19. DEFINITION. *Uniformization*(Γ_1, Γ_2) holds if for every $A \subseteq \mathcal{N}^2$, $A \in \Gamma_2$, there is a $B \subseteq A$, $B \in \Gamma_1$, such that

$$\forall \alpha [\exists \beta \langle \alpha, \beta \rangle \in A \leftrightarrow \exists \beta \langle \alpha, \beta \rangle \in B]$$

and, for every α there is at most one β with $\langle \alpha, \beta \rangle \in B$. (B is a *cross-section* or a *choice function* for A — see Fig. 2.) *Uniformization*(Γ) $\leftrightarrow$ *Uniformization*(Γ, Γ).

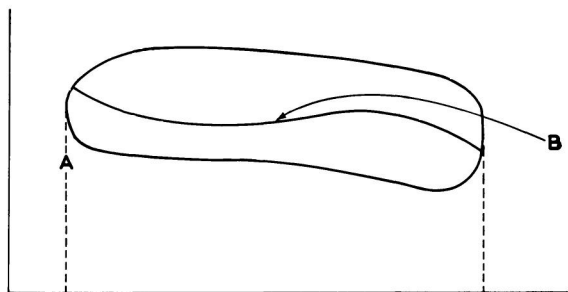


Fig. 2.

In terms of the effective theory, *Uniformization*(Γ) not only produces a basis for Γ , but also does so in a uniform way. But *Uniformization* makes sense for arbitrary pointclasses and is a classical notion, unlike the notion of basis.

4.20. THEOREM (Kondo–Addison–Novikov). *Uniformization*(Π_1^1). For all α , *Uniformization*($\Pi_1^1(\alpha)$).

4.21. COROLLARY. *Uniformization(Σ_2^1).*

4.22. COROLLARY. *Uniformization(Π_1^1); Uniformization(Σ_2^1).*

4.23. COROLLARY. Δ_2^1 is a basis for Σ_2^1 .

Corollary 4.22 is due to KONDO [1938] improving a result of Novikov (LUSIN and NOVIKOV [1935]). The effective version (i.e., the theorem) was proved by Addison who “effectivized” the earlier proofs.

We sketch the proof of the theorem. Let

$$A = \{ \langle \alpha, \beta \rangle : \forall \gamma \exists n R(\bar{\alpha}(n), \bar{\beta}(n), \bar{\gamma}(n)) \}.$$

Now let $X_{\alpha, \beta, R}$ be defined as before and set $|\sigma|_{\alpha, \beta} = |\sigma|^{<1 X_{\alpha, \beta, R}}$. Let $\phi : \omega \rightarrow \text{Seq}$ be recursive. Let

$$A_0 = A$$

$$A_{2n+1} = A_{2n} \cap \{ \langle \alpha, \beta \rangle : \forall \beta' (\langle \alpha, \beta' \rangle \in A_{2n} \rightarrow \beta(n) \leq \beta'(n)) \}.$$

$$A_{2n+2} = A_{2n+1} \cap \{ \langle \alpha, \beta \rangle : \forall \beta' (\langle \alpha, \beta' \rangle \in A_{2n+1} \rightarrow |\phi(n)|_{\alpha, \beta} \leq |\phi(n)|_{\alpha, \beta'} \\ \text{or } \phi(n) \notin X_{\alpha, \beta, R} \}$$

$$B = \bigcap_{n \in \omega} A_n.$$

Using ideas from the proof of Prewellordering(Π_1^1), one can show that $B \in \Pi_1^1$. The definition of A_{2n+1} guarantees that for each α there is at most one β with $\langle \alpha, \beta \rangle \in B$. If $\exists \beta (\langle \alpha, \beta \rangle \in A)$, then the definition of the A_n produces a unique candidate β for $\langle \alpha, \beta \rangle \in B$. Clearly for each n there is a β_n with $\langle \alpha, \beta_n \rangle \in A_{2n+2}$. If $\phi(n) \in X_{\alpha, \beta, R}$ set $\psi(\phi(n)) = |\phi(n)|_{\alpha, \beta_n}$. ψ is order preserving and so verifies $\langle \alpha, \beta \rangle \in B$.

The second half of the Theorem follows from the first half, using a Π_1^1 set universal for Π_1^1 . Corollary 4.22 follows from the second half of the Theorem and the relativization of Corollary 4.21.

To prove Corollary 4.21, let

$$\langle \alpha, \beta \rangle \in A \leftrightarrow \exists \gamma (\langle \alpha, \beta, \gamma \rangle \in C)$$

with $C \in \Pi_1^1$. By the Theorem, let $D \in \Pi_1^1$ give a cross-section for C , construing $\langle \beta, \gamma \rangle$ as an element of $\mathcal{N}$. Define B by

$$\langle \alpha, \beta \rangle \in B \leftrightarrow \exists \gamma (\langle \alpha, \beta, \gamma \rangle \in D).$$

For Corollary 4.23, let $A \in \Sigma_2^1$. Let $B = \{ \langle 0, \alpha \rangle : \alpha \in A \}$, where $0(n) = 0$ for all n . Let $C \in \Sigma_2^1$ be as given by Corollary 4.21. Then the unique α such that $\langle 0, \alpha \rangle \in C$ is given by

$$\begin{aligned}\alpha(n) = m &\leftrightarrow \exists \beta \langle (0, \beta) \in C \ \& \ \beta(n) = m \rangle \\ &\leftrightarrow \forall \beta \langle (0, \beta) \in C \rightarrow \beta(n) = m \rangle.\end{aligned}$$

The first condition shows $\alpha \in \Sigma_2^1$ and the second shows $\alpha \in \Pi_2^1$.

5. The axiom of constructibility and large cardinal axioms

Many basic question about projective sets cannot be settled on the basis of the ZFC axioms. It is consistent (if ZFC + there exists an inaccessible cardinal is consistent) that every projective set is measurable, has the Baire property, and has the perfect subset property (SOLOVAY [1970]). On the other hand, GÖDEL [1938] points out that, if the axiom of constructibility holds, then there is a set in Δ_2^1 which is not measurable and does not have the Baire property, and there is a set in Π_1^1 which does not have the perfect subset property. Whether or not the basic structural properties of Π_1^1 and Σ_2^1 , such as Prewellordering and Uniformization, hold for Π_n^1 , Σ_n^1 , or neither for $n \geq 3$ are similarly undecidable in ZFC. (This assertion should be weakened slightly. The consistency of, say, $\text{Prewellordering}(\Pi_n^1)$ is still unproved except for odd n , and there only from strong hypotheses.) Problems about relations between higher projective classes and Boolean algebraic operations appear similarly undecidable.

ADDISON [1959b] shows that most of the basic questions about projective sets can be answered by assuming the axiom of constructibility $V = L$.

If $V = L$, there is a wellordering $\triangleleft$ of $\mathcal{N}$ of order type ω_1 which belongs to Δ_2^1 . This well-ordering has a further technical property called “goodness”. This makes it possible to prove the following theorems:

5.1. THEOREM (Addison). *For all $n \geq 2$, $V = L \rightarrow \text{Prewellordering}(\Sigma_n^1)$ and so $\text{Prewellordering}(\Sigma_n^1)$.*

PROOF (outline). Let $A = \{\alpha : \exists \beta \langle \alpha, \beta \rangle \in B\}$ with $B \in \Pi_n^1$, $n \geq 1$. For each $\beta \in \mathcal{N}$, set $|\beta|$ = the order type of the initial segment of β with respect to $\triangleleft$. For $\alpha \in A$ set

$$\phi(\alpha) = \inf\{|\beta| : \langle \alpha, \beta \rangle \in B\}.$$

Using the “goodness” of $\triangleleft$, one can define the desired R and S . $\square$

5.2. THEOREM (Addison). *$V = L \rightarrow$ for every $n \geq 2$, $\text{Uniformization}(\Sigma_n^1)$ and so $\text{Uniformization}(\Sigma_n^1)$.*

The proof proceeds by choosing least elements in the sense of $\triangleleft$.

$V = L$ thus gives a fairly complete theory for projective sets. There are nevertheless two unpleasant aspects of this theory. As we have remarked, the regularity questions are all answered negatively. Furthermore, there is something odd about the sequence

$$\Sigma_0^1 \Pi_1^1 \Sigma_2^1 \Sigma_3^1 \Sigma_4^1 \cdots .$$

Solovay has shown that, if one assumes *large cardinal axioms* in place of $V = L$, some regularity questions about higher projective classes can be settled positively.

5.3. DEFINITION. A cardinal κ is *measurable* if there is a function μ defined on the power set of κ (κ is construed as a Von Neuman initial ordinal) such that

$$\mu(A) = 0 \text{ or } 1 \quad \text{for all } A;$$

$$\mu(\{\alpha\}) = 0 \quad \text{for all } \alpha < \kappa;$$

$$\mu(\kappa) = 1;$$

$$\mu(\kappa - A) = 1 - \mu(A);$$

$$\mu\left(\bigcup_{i \in I} A_i\right) = 0 \quad \text{if each } \mu(A_i) = 0 \text{ and } I \text{ has power } < \kappa.$$

5.4. DEFINITION. Let MC be the assertion that an uncountable measurable cardinal exists.

It is known that uncountable measurable cardinals, if they exist, must be very large. For example, if κ is an uncountable measurable cardinal, κ is the κ -th inaccessible cardinal. It is also known that MC does not follow from the ZFC axioms. Nevertheless, there are arguments — however inconclusive — to support the acceptance of MC and other large cardinal axioms.

5.5. THEOREM (Solovay). $MC \rightarrow$ every element of Σ_2^1 is measurable, has the Baire property, and has the perfect subset property (SOLOVAY [1969]).

Theorem 5.5 and the further results which follow are suprising, since an assumption about very large cardinal numbers is used to settle questions concerned only with $\mathcal{N}$ or the reals.

Some further progress can be made on structural questions if one assumes MC.

5.6. THEOREM (MANSFIELD [1971] improving a result of MARTIN and SOLOVAY [1969]). $MC \rightarrow \text{Uniformization}(\Pi_3^1, \Pi_2^1)$.

5.7. COROLLARY (MARTIN and SOLOVAY [1969]). $MC \rightarrow \Delta_4^1$ is a basis for Σ_3^1 .

Without much work one gets from the proof of the Corollary:

5.8. THEOREM (MARTIN [1977]). $MC \rightarrow$ every element of Σ_3^1 is a union of $\aleph_2$ Borel sets.

5.9. COROLLARY. Every element of Σ_3^1 has power $\leq \aleph_2$ or power $2^{\aleph_0}$.

Unhappily, MC does no more work. It is consistent with MC (Silver) that there is a set in Δ_3^1 which is not measurable and does not have the Baire property and that there is a set in Π_2^1 which does not have the perfect subset property. Furthermore MC seemingly does not allow us to settle whether Uniformization, or Prewellordering, or neither holds for Σ_3^1 or Π_3^1 . These results, mostly in SILVER [1971], are gotten by considering $L[\mu]$, the class of sets constructible from a μ which witnesses that some κ is measurable. Silver shows that in $L[\mu]$ there is a good wellordering of $\mathcal{N}$ which belongs to Δ_3^1 . He uses this wellordering just as Gödel and Addison use the wellordering $\triangleleft$ defined earlier.

6. Projective determinacy

There is little direct relation between structural properties and those regularity properties we have discussed. In GALE and STEWART [1953] a new regularity property was introduced: the property of *determinacy*. Results in MYCIELSKI and SWIERCZKOWSKI [1964] and DAVIS [1964], along with an old result of Banach, indicated that determinacy is stronger than the usual regularity properties in that it implies them all. Later, even more surprising results showed that determinacy implies even structural properties. In recent years it has become the custom to assume the determinacy of projective sets as an hypothesis and to deduce a theory of projective sets from this hypothesis.

6.1. DEFINITION. Let $A \subseteq \mathcal{N}$. Following GALE and STEWART [1953], associate with A a 2-person infinite game of perfect information $\mathcal{G}_A$. Player I begins the game by choosing $n_0 \in \omega$; then Player II chooses $n_1 \in \omega$; then I chooses $n_2 \in \omega$; and so on. Let $\alpha(i) = n_i$. I wins $\mathcal{G}_A$ just in case $\alpha \in A$. The notions of a *strategy* and of a *winning strategy* for I or II for $\mathcal{G}_A$ are defined in the obvious way. We say that $\mathcal{G}_A$ is *determined* if one of the players has a winning strategy. By *Determinacy*(Γ) we mean the assertion that $\mathcal{G}_A$ is determined for every $A \in \Gamma$. Projective determinacy (PD) is the assertion $\text{Determinacy}(\bigcup_n \Sigma_n^1)$.

6.2. THEOREM (Kechris, Martin improving results of Banach, Mycielski and Swierczkowski, and Morton Davis). *Determinacy*(Σ_n^1) $\rightarrow$ every set in Σ_{n+1}^1 is measurable, has the Baire property, and has the perfect subset property.

Just as with other regularity properties, one can prove determinacy for sufficiently simple classes, and MC makes possible a proof of determinacy for wider classes.

6.3. THEOREM (MARTIN [1975, 1970]). *Determinacy*(Δ_1^1). If MC, then *Determinacy*(Π_1^1) ($\leftrightarrow$ *Determinacy*(Σ_1^1)).

The proof of *Determinacy*(Δ_1^1) is quite different from the proofs of the other regularity properties of Borel sets. In other cases, the proofs can be carried out in the usual formal theory of ω and its power set. FRIEDMAN [1971] shows that *Determinacy*(Δ_1^1) cannot be proved in this theory and indeed cannot be proved in Zermelo set theory (set theory without the Axiom of Replacement). Hence, although *Determinacy*(Δ_1^1) is a statement about ω and $\mathcal{N}$ only, its proof involves in an essential way transfinite iterations of the power set operation.

Determinacy(Π_1^1) cannot be proved from the ZFC axioms, and even MC is not sufficient to prove *Determinacy*(Δ_2^1).

BLACKWELL [1967] showed that alternate proofs of some of the structural properties of Π_1^1 could be given using the Gale–Stewart theorem *Determinacy*(Σ_1^0) (GALE and STEWART [1953]). Addison and the author independently conceived of assuming PD and applying the method of Blackwell to higher projective classes. Moschovakis (ADDISON and MOSCHOVAKIS [1968]) and MARTIN [1968] independently proved the following theorem:

6.4. THEOREM. If PD, then *Prewellordering*(Σ_n^1) $\rightarrow$ *Prewellordering*(Π_{n+1}^1).

6.5. COROLLARY. *If PD, then Prewellordering(Π_n^1) for all odd n and Prewellordering(Σ_n^1) for all even n .*

6.6. COROLLARY. *If PD, then Prewellordering(Π_n^1) for all odd n and Prewellordering(Σ_n^1) for all even n .*

Corollary 6.5 follows from Theorems 6.4 and 3.8.

PROOF OF THEOREM 6.4. We give the proof from ADDISON and MOSCHOVAKIS [1968]. Let $A = \{\alpha : \forall \gamma \langle \alpha, \gamma \rangle \in B\}$ with $B \in \Sigma_n^1$. Let $\phi : B \rightarrow \text{Ordinals}$ be given by Prewellordering(Σ_n^1). For each $\beta \in A$ and $\alpha \in \mathcal{N}$ consider the following game $\mathcal{G}(\alpha, \beta)$: I and II choose $n_0, n_1, \dots$ by moving alternately. Let $\gamma(i) = n_{2i}$ and $\delta(i) = n_{2i+1}$. I wins if

$$\alpha \notin A \quad \text{or} \quad \phi(\langle \alpha, \gamma \rangle) > \phi(\langle \beta, \delta \rangle).$$

We define a relation $\alpha \leq \beta$ by

$$\alpha \leq \beta \leftrightarrow \text{II has a winning strategy for } \mathcal{G}(\alpha, \beta).$$

Since $\mathcal{G}(\alpha, \beta) = \mathcal{G}_C$ for projective C , PD implies that $\mathcal{G}(\alpha, \beta)$ is determined. This justifies the following, for $\beta \in A$:

$$\alpha \leq \beta \leftrightarrow \exists s \forall \gamma (s \text{ is a strategy for II \&}$$

$$\langle \alpha, \gamma \rangle \in B \text{ \& } \phi(\langle \alpha, \gamma \rangle) \leq \phi(\langle \beta, s(\gamma) \rangle)).$$

$$\beta \not\leq \alpha \leftrightarrow \exists s \forall \gamma (s \text{ is a strategy for I \&}$$

$$\langle \alpha, \gamma \rangle \in B \text{ \& } \phi(\langle \alpha, \gamma \rangle) < \phi(\langle \beta, s(\gamma) \rangle)).$$

The expressions on the right define relations in Σ_{n+1}^1 . Also, $\alpha \leq \alpha$, since II can simply choose $\delta = \gamma$.

If $\alpha \not\leq \beta$, then I has a winning strategy s for $\mathcal{G}(\alpha, \beta)$. Hence $\alpha \notin A$ or II has a winning strategy s' for $\mathcal{G}(\beta, \alpha)$ defined by $s'(\langle n_2, \dots, n_k \rangle) = s(\langle n_1, \dots, n_{k-1} \rangle)$. This shows that, for α and $\beta \in A$,

$$\alpha \not\leq \beta \Rightarrow \beta \leq \alpha.$$

Suppose $\alpha \leq \beta \leq \gamma$. Let s_1 and s_2 be strategies for II witnessing $\alpha \leq \beta$ and $\beta \leq \gamma$ respectively. Let $s_3 = s_2 s_1$. Then s_3 is a strategy for II witnessing $\alpha \leq \gamma$.

Say $\alpha > \beta \leftrightarrow \alpha \not\leq \beta$. Suppose $\alpha_0 > \alpha_1 > \alpha_2 > \dots$. Let $s_0, s_1, \dots$ be winning strategies for I for the games $\mathcal{G}(\alpha_0, \alpha_1), \mathcal{G}(\alpha_1, \alpha_2), \dots$ respectively. We produce simultaneously plays of all the $\mathcal{G}(\alpha_i, \alpha_{i+1})$ by letting I's moves in $\mathcal{G}(\alpha_i, \alpha_{i+1})$ be as dictated by s_i and II's moves in $\mathcal{G}(\alpha_i, \alpha_{i+1})$ be I's moves in

$\mathcal{G}(\alpha_{i+1}, \alpha_{i+2})$. The resulting play yields a sequence $\gamma_0, \gamma_1, \dots$ such that each $\langle \alpha_i, \gamma_i \rangle \in B$ and

$$\phi(\langle \alpha_0, \gamma \rangle) > \phi(\langle \alpha_1, \gamma_1 \rangle) > \dots$$

This is a contradiction.

We have shown that $\leq$ is reflexive, connected and transitive and the associated $<$ is well-founded. Hence there is a $\psi : A \rightarrow \text{Ordinals}$ such that $\alpha \leq \beta \leftrightarrow \psi(\alpha) \leq \psi(\beta)$. $\square$

The problem of proving Uniformization(Π_n^1) for all odd n from PD was open for some time. Then Moschovakis formulated and proved a stronger result.

6.7. DEFINITION. *Scale(Γ)* means that, for every $A \in \Gamma$, $A \subseteq \mathcal{N}$, there is a sequence ϕ_i, R_i, S_i , $i = 0, 1, 2, \dots$, such that the following hold.

$$(i) \quad \{\langle i, \alpha, \beta \rangle : \langle \alpha, \beta \rangle \in R_i\} \in \check{\Gamma}; \quad \{\langle i, \alpha, \beta \rangle : \langle \alpha, \beta \rangle \in S_i\} \in \check{\Gamma}.$$

(ii) Each A, ϕ_i, R_i, S_i has the properties demanded of A, ϕ, R, S in the definition of Prewellordering (Definition 3.3).

(iii) Suppose $\alpha_n \in A$, $n = 0, 1, 2, \dots$, $\alpha = \lim_n \alpha_n$, and for every i the sequence $\phi_i(\alpha_0), \phi_i(\alpha_1), \dots$ is eventually constant. Then

$$(a) \quad \alpha \in A;$$

$$(b) \quad \forall i (\phi_i(\alpha) \leq \lim_n \phi_i(\alpha_n)).$$

6.8. THEOREM (MOSCHOVAKIS [1971]). *Scale(Π_n^1) $\rightarrow$ Scale(Σ_{n+1}^1). If PD, then Scale(Σ_n^1) $\rightarrow$ Scale(Π_{n+1}^1).*

The proof of the more difficult second part is by an extension of the methods of the proof of Theorem 6.4.

6.9. COROLLARY. *Assume PD. Scale(Π_n^1) and Scale(Π_n^1) for n odd; Scale(Σ_n^1) and Scale(Σ_n^1) for n even.*

Corollary 6.9 follows from Theorem 6.4 and the easily proved Scale(Σ_1^0).

6.10. COROLLARY. *Assume PD. Uniformization(Π_n^1) and Uniformization(Π_n^1) for n odd; Uniformization(Σ_n^1) and Uniformization(Σ_n^1) for n even, $n > 0$.*

PROOF. The proof of Corollary 6.10 is exactly like that of Theorem 4.20, with $\phi_n(\alpha, \beta)$ playing the role played there by $|\phi(n)|_{\alpha, \beta}$. $\square$

6.11. COROLLARY. *If PD, then Δ_n^1 is a basis for Σ_n^1 for all even n .*

From Theorems 6.4 and 6.8, and a further result of MOSCHOVAKIS [1973] proved by a similar method, researchers have deduced an almost complete structural theory for the projective hierarchy. Projective determinacy is then at least equal to $V = L$ in strength with respect to questions about projective sets, and it is more pleasing in that (1) regularity questions are answered positively and (2) the sequence

$$\Sigma_0^1 \Pi_1^1 \Sigma_2^1 \Pi_3^1 \cdots$$

seems more plausible than that derived from $V = L$.

PD also sheds light on the question of the relation between projection and Boolean algebraic operations.

6.12. DEFINITION. δ_n^1 is the least ordinal not the length of a well-founded relation on $\mathcal{N}$ belonging to Δ_n^1 .

6.13. DEFINITION. If κ is a cardinal number, $A \subseteq \mathcal{N}$ is κ -Souslin if there is a relation R such that

$$\alpha \in A \leftrightarrow \exists f: \omega \rightarrow \kappa \forall n R(\bar{\alpha}(n), \bar{f}(n)).$$

6.14. THEOREM. A is $\aleph_0$ -Souslin $\leftrightarrow A \in \Sigma_1^1$. $A \in \Sigma_2^1 \rightarrow A$ is $\aleph_1$ -Souslin (SHOENFIELD [1961]). If MC, then $A \in \Sigma_3^1 \rightarrow A$ is $\aleph_2$ -Souslin (MARTIN, based on MARTIN and SOLOVAY [1969]). If PD, then $A \in \Sigma_{2n+2}^1 \rightarrow A$ is κ -Souslin where κ is the cardinal of δ_{2n+1}^1 (Moschovakis). If PD, then $A \in \Sigma_{2n+1}^1 \rightarrow A$ is κ -Souslin for some $\kappa < \delta_{2n+1}^1$ (Moschovakis).

For Σ_1^1 , the result is by Theorem 2.16. The proof of Theorem 2.23 gives a representation of sets in Σ_2^1 as $\aleph_1$ -Souslin. The last two sentences of the Theorem follow from Theorem 6.8.

6.15. THEOREM (Kunen, MARTIN [1977]). *Every κ -Souslin well-founded relation has length of power $\leq \kappa$, if κ is infinite.*

6.16. COROLLARY. $\delta_2^1 \leq \omega_2$ (MARTIN [1977]). $MC \rightarrow \delta_3^1 \leq \omega_3$. $PD \rightarrow \delta_4^1 \leq \omega_4$.

6.17. COROLLARY. *If PD, then $A \in \Sigma_4^1 \rightarrow A$ is a union of $\aleph_3$ Borel sets.*

Some of the most interesting open questions regarding determinacy and projective sets concern the δ_n^1 . What are upper bounds for δ_n^1 , $n \geq 5$?

Kunen has some partial results for $n = 5$. Are the δ_n^1 cardinals? The latter question is not a purely technical one, since the continuum hypothesis implies that, for $n \geq 2$, $\omega_1 < \delta_n^1 < \omega_2$.

As a final application of projective determinacy, we mention the *Wadge ordering*.

6.18. DEFINITION. If $A, B \subseteq \mathcal{N}$, $A \leq_w B$ just in case there is a continuous $f: \mathcal{N} \rightarrow \mathcal{N}$ such that $f(A) \subseteq B$ and $f(\bar{A}) \subseteq \bar{B}$.

6.19. THEOREM (W. Wadge). Assume PD. If A and B are projective, then $A \leq_w B$ or $B \leq_w \bar{A}$.

PROOF. Consider the game G defined as follows. Let α be I's play and let β be II's play. II wins just in case

$$\alpha \in A \leftrightarrow \beta \in B.$$

A winning strategy for II witnesses $A \leq_w B$. A winning strategy for I witnesses $B \leq_w \bar{A}$.

6.20. DEFINITION. If $A, B \subseteq \mathcal{N}$, $A \sim_w B$ if $(A \leq_w B \text{ and } B \leq_w A)$ or $(A \leq_w \bar{B} \text{ and } \bar{B} \leq_w A)$. The *Wadge degree* of $A = [A] = \{B: A \sim_w B\}$. $[A] < [B] \leftrightarrow A \leq_w B \text{ and } A \not\leq_w B$.

6.21. THEOREM (Martin). If PD, then the Wadge degrees of projective sets are well-ordered by $<$.

Remark. Theorem 6.19 already gives that the Wadge degrees are linearly ordered.

The Wadge degrees are thus an ultimately fine hierarchy on the projective sets, assuming PD. If more determinacy than PD is assumed, this Wadge hierarchy extends correspondingly further. For Borel sets, no determinacy assumption is required, by Theorem 6.3.

Call a Wadge degree $[A]$ self-dual if $A \leq_w \bar{A}$. Steel has shown from, say, PD that Reduction must hold on one side or other of any, say, projective non-self-dual Wadge degree closed under countable unions and intersections. This helps to explain the empirically observed pervasiveness of the Reduction phenomenon.

We now discuss briefly some of the consequences of a demonstrably false proposition.

6.22. DEFINITION. The *axiom of determinacy* (AD) is the assertion that $\mathcal{G}_A$ is determined for every A .

AD was proposed by Mycielski and Steinhaus. See MYCIELSKI [1964] for more information on AD. AD contradicts the axiom of choice and so is not a genuine candidate for an axiom of set theory. Nevertheless consequences of AD are worth noting because AD may hold, for example, in the realm of sets ordinal definable from reals.

AD implies that *all* sets have all important regularity properties. For example, AD implies that every set is measurable (MYCIELSKI and SWIERCZKOWSKI [1964]), has the Baire property, and has the perfect subset property (DAVIS [1964]).

AD implies that the collection of all Wadge degrees is well-ordered, and thus the entire power set of the continuum is arranged in a hierarchy of increasing complexity.

In the area of projective sets, AD has some very appealing consequences, consequences mostly inconsistent with the axiom of choice. AD implies that the δ_n^1 are all cardinals (MOSCHOVAKIS [1970]), in fact, measurable cardinals (Kunen, Martin, Solovay).

6.23. DEFINITION. If κ is a cardinal $\mathbf{B}_\kappa$ is the smallest Boolean algebra containing the open sets and closed under well-ordered unions and intersections of length $< \kappa$.

6.24. THEOREM (MARTIN [1977], MOSCHOVAKIS [1971]). $AD \rightarrow \mathbf{B}_{\delta_n^1} = \Delta_n^1$ for all odd n .

For $n = 1$, the conclusion is just the Souslin Theorem 1. $\Delta_n^1 \subseteq \mathbf{B}_{\delta_n^1}$ for odd n is a consequence of PD and so apparently is not inconsistent with the axiom of choice. Even $\Delta_3^1 \supseteq \mathbf{B}_{\delta_3^1}$ is inconsistent with MC plus the axiom of choice. Thus AD gives a more elegant descriptive set theory than is possible with the axiom of choice. This is even more striking when one considers Σ_n^2 , defined by projection on the power set of $\mathcal{N}$. AD gives a very pleasant theory of these classes, and no significant structural theory consistent with the axiom of choice is known.

Is PD true? It is certainly not self-evident. Some set theorists consider large cardinal axioms self-evident, or at least as following from *a priori* principles implied by the concept of set. Weak forms of PD (Determinacy(Π_1^1)) follows from large cardinal axioms. It is possible that PD itself follows from large cardinal axioms, but this remains unproved.

The author regards PD as an hypothesis with a status similar to that of a theoretical hypothesis in physics. Three kinds of quasi-empirical evidence for PD have been produced.

- (1) The mere failure to refute such a powerful assertion is some evidence for its truth.
- (2) Special cases of PD have been verified: Determinacy(Δ_1^1).
- (3) The consequences of PD in the realm of descriptive set theory are so plausible and coherent that they lend plausibility to the principle which implies them.

References

- ADDISON, J.W.
 [1959a] Separation principles in the hierarchies of classical and effective descriptive set theory, *Fund. Math.*, **46**, 123–135.
 [1959b] Some consequences of the axiom of constructibility, *Fund. Math.*, **46**, 337–357.
- ADDISON, J.W. and Y.N. MOSCHOVAKIS
 [1968] Some consequences of the axiom of definable determinateness, *Proc. Nat. Acad. Sci. U.S.A.*, **59**, 708–712.
- BLACKWELL, D.
 [1967] Infinite games and analytic sets, *Proc. Nat. Acad. Sci. U.S.A.*, **58**, 1836–1837.
- COHEN, P.J.
 [1963] The independence of the continuum hypothesis I, *Proc. Nat. Acad. Sci. U.S.A.*, **50**, 1143–1148.
 [1964] The independence of the continuum hypothesis II, *Proc. Nat. Acad. Sci. U.S.A.*, **50**, 105–110.
- DAVIS, MORTON
 [1964] Infinite games of perfect information, in: *Advances in Game Theory*, Annals of Mathematics Studies, Vol. 52 (Princeton University Press, Princeton, NJ) pp. 85–101.
- FRIEDMAN, H.
 [1971] Higher set theory and mathematical practice, *Annals of Math. Logic*, **2**, 326–357.
- GALE, D. and F.M. STEWART
 [1953] Infinite games with perfect information, in: *Contributions to the Theory of Games*, Annals of Mathematics Studies, Vol. 28 (Princeton University Press, Princeton, NJ) pp. 245–266.
- GÖDEL, K.
 [1938] The consistency of the axiom of choice and of the generalized continuum hypothesis, *Proc. Nat. Acad. Sci. U.S.A.*, **24**, 556–557.
 [1940] *The Consistency of the Axiom of Choice and of the Generalized Continuum Hypothesis with the Axioms of Set Theory*, Annals of Mathematics Studies, Vol. 3 (Princeton University Press, Princeton, NJ).
- KLEENE, S.C.
 [1952] *Introduction to Metamathematics* (North-Holland, Amsterdam).
 [1955] Arithmetical predicates and function quantifiers, *Trans. Am. Math. Soc.*, **79**, 312–340.
- KONDO, M.
 [1938] Sur l'uniformisation des complémentaires analytiques et les ensembles projectifs de la seconde classe, *Japan J. Math.*, **15**, 197–230.

LEBESGUE, H.

- [1905] Sur les fonctions representable analytiquement, *J. de Math.*, 6^e série, **1**, 139–216.

LUSIN, N.

- [1917] Sur la classification de M. Baire, *C.R. Acad. Sci. Paris*, **164**, 91–94.
 [1925] Sur les ensembles projectifs de M. Henri Lebesgue, *C.R. Acad. Sci. Paris*, **180**, 1572–1574.

LUSIN, N. and P. NOVIKOV

- [1935] Choix effectif d'un point dans un complémentaire analytique arbitraire, donné par un crible, *Fund. Math.* **25**, 559–560.

LUSIN, N. and W. SIERPINSKI

- [1923] Sur un ensemble non mesurable B, *J. de Math.*, 7^e série, **2**, 53–72.

MANSFIELD, R.

- [1971] A Souslin operation for Π_2^1 , *Israel J. Math.*, **9** (3), 367–369.

MARTIN, D.A.

- [1968] The axiom of determinateness and reduction principles in the analytical hierarchy, *Bull. Am. Math. Soc.*, **74**, 687–689.
 [1970] Measurable cardinals and analytic games, *Fund. Math.*, **66**, 287–291.
 [1975] Borel determinacy, *Ann. of Math.*, **102**, 363–371.
 [1977] Projective sets and cardinal numbers, *J. Symbolic Logic*, to appear.

MARTIN, D.A. and R.M. SOLOVAY

- [1969] A basis theorem for Σ_1^1 sets of reals, *Ann. of Math.*, **89**, 138–160.

MOSCHOVAKIS, Y.N.

- [1970] Determinacy and prewellorderings of the continuum, in: *Mathematical Logic and Foundations of Set Theory*, edited by Y. Bar-Hillel (North-Holland, Amsterdam) pp. 24–62.
 [1971] Uniformization in a playful universe, *Bull. Am. Math. Soc.*, **77**, 731–736.
 [1973] Analytical definability in a playful universe, in: *Logic, Methodology and Philosophy of Science IV*, edited by P. Suppes et al. (North-Holland, Amsterdam) pp. 77–85.
 [1978] *Descriptive Set Theory* (North-Holland, Amsterdam) to appear.

MYCIELSKI, J.

- [1964] On the axiom of determinateness, *Fund. Math.*, **53**, 204–224.

MYCIELSKI, J. and S. SWIERCZKOWSKI

- [1964] On the Lebesgue measurability and the axiom of determinateness, *Fund. Math.*, **54**, 67–71.

SHOENFIELD, J.R.

- [1961] The problem of predicativity, in: *Essays on the Foundations of Mathematics*, dedicated to A.A. Fraenkel, edited by Y. Bar-Hillel et al. (Magnes Press, Jerusalem) pp. 132–139.

SIERPINSKI, W.

- [1925] Sur une classe d'ensembles, *Fund. Math.*, **7**, 237–243.

SILVER, J.H.

- [1971] Measurable cardinals and Δ_1^1 well-orderings, *Ann. of Math.*, **94**, 414–446.

SOLOVAY, R.M.

- [1969] On the cardinality of Σ_2^1 sets of reals, in: *Foundations of Mathematics* (Springer, Berlin) pp. 58–73.
 [1970] A model of set-theory in which every set of reals is Lebesgue measurable, *Ann. of Math.*, **92**, 1–56.

PART D

*Proof Theory and Constructive
Mathematics*

Guide to Part D: *Proof Theory and Constructive Mathematics*

with the cooperation of
A. TROELSTRA

D.1. SMORYNSKI	
<i>The Incompleteness Theorems</i>	821
D.2. SCHWICHTENBERG	
<i>Proof theory: Some applications of cut-elimination</i>	867
D.3. STATMAN	
<i>Herbrand's Theorem and Gentzen's notion of a direct proof</i>	897
D.4. FEFERMAN	
<i>Theories of finite type related to mathematical practice</i>	913
D.5. TROELSTRA	
<i>Aspects of constructive mathematics</i>	973
D.6. FOURMAN	
<i>The logic of topoi</i>	1053
D.7. BARENDREGT	
<i>The type free lambda calculus</i>	1091
D.8. PARIS and HARRINGTON	
<i>A mathematical incompleteness in Peano arithmetic</i>	1133

The mathematician constructs proofs. The proof-theorist considers proofs themselves as mathematical objects and studies them with the tools of modern mathematics.

Proof theory began with Hilbert's Program. Hilbert's idea was to exploit the concrete, finitistic nature of proofs to provide a simple foundation for mathematics. Gödel's Incompleteness Theorems dealt the program a staggering blow. These theorems are among the most basic in logic and are discussed in Smorynski's introductory chapter.

It was much harder to make a reasonable selection of topics from proof theory than from the other parts of logic because the subject is going in many different directions. We attempted to select topics which illustrate the parts of proof theory which are well developed and are relevant to

other parts of logic and mathematics. Reading the chapters that resulted one sees certain threads which run through them and seem to be central concerns of present-day proof theory. We mention two.

One of the most important threads holding proof theory together is the question: What more do we know about a *true* statement when we learn that it is *provable* in a particular theory, or has a proof in some normal form? Another is the search for relationships between mathematical and proof-theoretic principles. Both of these aspects of proof theory are beautifully illustrated in Schwichtenberg's chapter. He shows the reader how Gentzen's method of cut-elimination can be used for a wide variety of such studies.

The first thread mentioned above is central to Statman's chapter. He presents a case study of what more one can learn from a direct proof of a theorem in a formal equation calculus than one learns from an indirect proof.

Feferman's chapter looks at some formal theories of higher-type mathematical objects, functions on natural numbers, sets of such functions, etc. These theories must, by Gödel's Theorem, be incomplete but empirical evidence shows that they embody natural mathematical principles and are strong enough to carry out large portions of mathematics. Feferman studies the above questions as well as the relative strength of the various theories by means of independence results.

Troelstra's chapter discusses constructive notions of proof. Consider, for example, a proof of $\varphi \vee \psi$ (" φ or ψ "). A classical mathematician accepts a proof of $\varphi \vee \psi$ even when the proof does not tell him which of the two is actually true. (Take $\varphi \vee \neg \varphi$ for example.) The constructivist demands more. For him a proof of $\varphi \vee \psi$ must contain either a proof of φ or a proof of ψ and he must be able to tell which. Beyond such simplicities, however, lie highly problematic matters. The study of constructive proofs gives rise to several competing, and mutually incompatible, views of constructive mathematics, *intuitionism* being one of the best known.

Fourman's chapter discusses the relationship between intuitionism and the notion of *topos* from category theory. The Kock-Reyes chapter (Chapter A.8) gave the category-theorist's view of parts of logic. Here we get the logicians view of parts of category theory. The Barendregt chapter discusses recent progress in the old search for a coherent theory of self-applicable functions.

The Handbook comes to a dramatic close with the Paris-Harrington chapter which discusses a true statement of finite combinatorics which is not provable in Peano arithmetic.

The Incompleteness Theorems

C. SMORYNSKI

Contents

1. Hilbert's Program	822
2. Gödel's theorems	825
2.1. Preliminaries	826
2.2. Proof of the Incompleteness Theorems	827
2.3. Things to come	829
3. Encoding	829
3.1. Primitive recursive encoding of finite sequences	831
3.2. Primitive recursive encoding of syntax	835
3.3. Rosser's Theorem	840
*3.4. Recursion theory	841
*3.5. The formula hierarchy	843
4. Metamathematical properties other than consistency	844
4.1. Reflection principles	844
*4.1 ^a . Hierarchy considerations	849
*4.2. ω -consistency	851
4.3. Completeness properties	854
*4.3 ^a . Kent's Theorem	855
5. Two applications	856
5.1. A fix-point theorem	856
5.2. Conservation results	858
*6. The formalized completeness theorem	860
*6.1. The Hilbert–Bernays Completeness Theorem	860
*6.2. The incompleteness theorems	861
*6.3. Comments	863
References	864

* This subsection covers an advanced topic

1. Hilbert's Program

Mathematics, at the turn of the century, was plagued by various difficulties ranging from antinomies and paradoxes to inconsistencies both formal and personal. There had been difficulties earlier in mathematics, but these had been removed or detoured: The Greeks eventually shrugged their shoulders and admitted irrational numbers; the analysts avoided paradoxes involving infinitesimals by finally isolating and rigorizing the concepts of limit and continuity. Even in set theory, the solution to the problem of the paradoxes had been offered as early as 1908 by Zermelo: One must first know what one is talking about before one can axiomatize a subject. Thus, instead of taking as axioms for set theory some intuitively obvious properties of finite sets, some obvious properties of the set of all subsets of a given set, and yet some other obvious properties of a third entity — a process that almost guarantees contradictions — Zermelo first described the cumulative hierarchy and then listed axioms for this *single* entity. Until recent work on large cardinals, axioms later added were merely further properties obviously true for this hierarchy but which were formally underivable.

Sociologists would describe what transpired next in terms of “culture lag”. Despite the fact that a consistent set theory was available, mathematicians continued to worry about consistency. Some even doubted the consistency of arithmetic itself! To make matters worse, L.E.J. Brouwer was making the rounds in a bizarre attempt to turn mathematics into a religion.

When, in 1920, Hermann Weyl fell prey to Brouwer's lunacy, David Hilbert decided to intervene. He observed that (REID [1970] p. 155) “What Weyl and Brouwer do comes to the same thing as to follow in the footsteps of Kronecker! They seek to save mathematics by throwing overboard all that which is troublesome They would chop up and mangle the science. If we would follow such a reform as the one they suggest, we would run the risk of losing a great part of our most valuable treasures!”

The vehemence with which Hilbert made the above declaration is most readily understood when one remembers that Hilbert made his name by the use of non-constructive techniques. His solution to Gordon's problem in the theory of invariants (REID [1970], Chapter V) had elicited the charge of “theology” from Gordon. Kronecker refused to believe that the theorem, which asserted the existence of objects satisfying some condition, had been proven as the objects had not been explicitly constructed. Lindemann called the technique “unheimlich”. Thus, it is not surprising

that Hilbert continued (REID [1970], p. 157) "I believe that as little as Kronecker was able to abolish the irrational numbers . . . just as little will Weyl and Brouwer today be able to succeed. Brouwer is not, as Weyl believes him to be, the Revolution — only the repetition of an attempted Putsch".

Even if Hilbert had faith in Zermelo's set theory, he could not use it: For, he had not to secure mathematics but to stop a Putsch. So Hilbert proposed his Conservation Program: To justify the use of abstract techniques, he would show — by as simple and concrete a means as possible — that the use of abstract techniques was *conservative* — i.e. that any concrete assertion one could derive by means of such abstract techniques would be derivable without them.

To clarify these matters, we introduce some Hilbertian jargon whose exact meaning was never delineated by Hilbert. First, in the domain of concrete mathematics, there are *finitistically meaningful* statements and *finitistic* means of proof. The finitistically meaningful statements are called *real* statements and are (say) identities of the form

$$\forall x (fx = gx),$$

where f, g are reasonably simple functions (e.g. primitive recursive). Finitistic proofs correspond roughly to computations or combinatorial manipulations. More complicated statements are merely *ideal* ones and, as such, have no meaning; but they can be manipulated abstractly — just as i is not a real number, but can be dealt with algebraically, freely using the fact that $i^2 = -1$. Hilbert's contention was that, just as the use of i leads to no new algebraic identities, the use of ideal statements and abstract reasoning about them would not allow one to derive any new real statements — i.e. none which were not already derivable finitistically. To refute Weyl and Brouwer, Hilbert required that this latter conservation property itself be finitistically provable.

To avail itself of a finitistic treatment, the ideal statements and abstract reasoning would have to be codified in some formal system. Then the abstract reasoning would be codified by simple combinatorial manipulations and similar simple combinatorial manipulations could be used to demonstrate this conservation.

At this point, one could try to analyze either the reasons for Hilbert's belief that this could be done or the assumptions that necessarily underly such a Program. The author does not find these topics particularly interesting and so we skip them.

The question probably on the reader's mind is: This is all very nice, but

where does *consistency* come in? For, as everyone knows, this chapter is supposed to be about consistency. Hilbert's Consistency Program is a natural outgrowth of and successor to Hilbert's Conservation Program. There are two reasons for this:

(i) Consistency is merely the assertion that some string of symbols is not derivable. Since derivations are simple combinatorial manipulations, this is a finitistically meaningful statement and ought to have a finitistic proof.

(ii) Proving consistency of the formal system encoding the abstract concepts already establishes the conservation result!

Reason (i) is straightforward and we do not discuss it. Reason (ii) is particularly important and we should comment on it. Let **R**, **I** denote formal systems encoding real statements with their finitistic proofs and ideal systems with their abstract reasoning, respectively. Let φ be a real statement $\forall x (fx = gx)$. Now, if $\mathbf{I} \vdash \varphi$, then there is a derivation, d , of φ from **I**. But, derivations are concrete objects and, for some real formula $P(x, y)$ encoding derivations in **I**,

$$\mathbf{R} \vdash P(d, \ulcorner \varphi \urcorner),$$

where $\ulcorner \varphi \urcorner$ is some code for φ . Now, if φ were false, one would have $fa \neq ga$ for some a and hence,

$$\mathbf{R} \vdash P(c, \ulcorner \neg \varphi \urcorner)$$

for some c . In fact, one would have the stronger assertion

$$\mathbf{R} \vdash fx \neq gx \rightarrow P(c_x, \ulcorner \neg \varphi \urcorner)$$

for some c_x depending on x . But, if **R** proves consistency of **I**, we see

$$\mathbf{R} \vdash \neg (P(d, \ulcorner \varphi \urcorner) \wedge P(c, \ulcorner \neg \varphi \urcorner)),$$

whence $\mathbf{R} \vdash fx = gx$, with free variable x , i.e. $\mathbf{R} \vdash \forall x (fx = gx)$.

[The above argument is a bit vague and is rife with additional assumptions. To make it rigorous, we would have to get down to the basics of encoding — which is more than we intend to do in this section. The assumptions on P are brought out in Sections 2 and 3. A formal version of the above argument appears in Section 4.]

The argument of the above paragraph clearly invited Hilbert to establish his Consistency Program: To devise a finitistic means of proving the consistency of various formal systems encoding abstract reasoning with ideal statements.

Since the Consistency Program was as broad as the general Conservation Program and, since it looked more tractable, Hilbert fixed on it, asserting (MESCHKOWSKI [1973], p. 56):

If the arbitrarily given axioms do not contradict each other through their consequences, then they are true, then the objects defined through the axioms exist. That, for me, is the criterion of truth and existence.

In summary, Hilbert's Consistency Program had as its goal the proof, by finitistic means, of the consistency of strong systems. The solution would completely justify the use of abstract concepts. The proof would successfully repudiate Brouwer and bring Weyl back into the fold.

It's a shame that it couldn't work.

2. Gödel's theorems

In 1930, while in his twenties, Kurt Gödel made a major announcement: Hilbert's Consistency Program could not be carried out. For, he had proven two theorems which were then considered moderately devastating and which still induce nightmares among the infirm. Loosely stated, these theorems are:

FIRST INCOMPLETENESS THEOREM. *Let $\mathbf{T}$ be a formal theory containing arithmetic. Then there is a sentence φ which asserts its own unprovability and is such that:*

- (i) *If $\mathbf{T}$ is consistent, $\mathbf{T} \not\vdash \varphi$.*
- (ii) *If $\mathbf{T}$ is ω -consistent, $\mathbf{T} \not\vdash \neg \varphi$.*

SECOND INCOMPLETENESS THEOREM. *Let $\mathbf{T}$ be a consistent formal theory containing arithmetic. Then*

$$\mathbf{T} \not\vdash \text{Con}_{\mathbf{T}},$$

where $\text{Con}_{\mathbf{T}}$ is the sentence asserting the consistency of $\mathbf{T}$.

The Second Theorem clearly destroys the Consistency Program. For, if $\mathbf{R}$ cannot prove its own consistency, how can it hope to prove the consistency of $\mathbf{I}$? ($\mathbf{R}$ and $\mathbf{I}$ are as in Section 1.) Even the First Theorem does this since (1) the statement φ is real; and (2) φ is easily seen to be true. ((1) requires looking at the construction of φ ; (2) is seen by observing that φ asserts its unprovability and is indeed unprovable.) Thus, the First Theorem shows that the Conservation Program cannot be carried out and, hence, that the same must hold for the Consistency Program.

Let us consider the proofs of these remarkable theorems.

2.1. Preliminaries

The clause in each theorem that **T** contain arithmetic is just a means of avoiding the problem of stating explicitly what conditions must be met. These conditions are encodability conditions and, as Gödel showed, one can do a great deal of encoding on natural numbers. We defer until Section 3 the discussion of *how* the encoding is handled and discuss here *what* is to be encoded and *where* it is to be encoded.

Throughout this chapter, **T** will be some fixed, but unspecified, consistent formal theory. For later convenience, we assume that the encoding is done in some fixed formal theory **S** and that **T** contains **S**. We do not specify **S** — it is usually taken to be a formal system of arithmetic, although a weak set theory is often more convenient. The sense in which **S** is contained in **T** is better exemplified than explained: If **S** is a formal system of arithmetic and **T** is, say, **ZF**, then **T** contains **S** in the sense that there is a well-known embedding, or *interpretation*, of **S** in **T**. It is this sort of embedding that we have in mind.

Since encoding is to take place in **S**, it will have to have a large supply of constants and closed terms to be used as codes. (E.g. in formal arithmetic, one has $\bar{0}, \bar{1}, \dots$) **S** will also have certain function symbols to be described shortly.

To each formula, φ , of the language of **T** is assigned a closed term, $\ulcorner \varphi \urcorner$, called the *code* of φ . [N.B. If φx is a formula with free variable x , then $\ulcorner \varphi x \urcorner$ is a closed term encoding the formula φx , with x viewed as a *syntactic object* and not as a parameter.] Corresponding to the logical connectives and quantifiers are function symbols, neg, imp, etc., such that, for all formulae φ, ψ , $\mathbf{S} \vdash \text{neg}(\ulcorner \varphi \urcorner) = \ulcorner \neg \varphi \urcorner$, $\mathbf{S} \vdash \text{imp}(\ulcorner \varphi \urcorner, \ulcorner \psi \urcorner) = \ulcorner \varphi \rightarrow \psi \urcorner$, etc.

Of particular importance is the substitution operator, represented by the function symbol sub. For formulae φx , terms t with codes $\ulcorner t \urcorner$,

$$\mathbf{S} \vdash \text{sub}(\ulcorner \varphi x \urcorner, \ulcorner t \urcorner) = \ulcorner \varphi t \urcorner.$$

Iteration of sub allows one to define $\text{sub}_3, \text{sub}_4, \dots$, such that

$$\mathbf{S} \vdash \text{sub}_n(\ulcorner \varphi x_1 \cdots x_n \urcorner, \ulcorner t_1 \urcorner, \dots, \ulcorner t_n \urcorner) = \ulcorner \varphi t_1 \cdots t_n \urcorner.$$

Finally, we also encode derivations and have a binary relation $\text{Prov}_{\mathbf{T}}(x, y)$ (read “ x proves y ” or “ x is a proof of y ”) such that for closed t_1, t_2 : $\mathbf{S} \vdash \text{Prov}_{\mathbf{T}}(t_1, t_2)$ iff t_1 is the code of a derivation in **T** of the formula with code t_2 . It follows that $\mathbf{T} \vdash \varphi$ iff $\mathbf{S} \vdash \text{Prov}_{\mathbf{T}}(t, \ulcorner \varphi \urcorner)$ for some closed term t .

If one defines

$$\text{Pr}_{\mathbf{T}}(y) \leftrightarrow \exists x \text{Prov}_{\mathbf{T}}(x, y),$$

then one obtains a predicate asserting provability. However, it is *not* always the case that

$$(*) \quad \mathbf{T} \vdash \varphi \quad \text{iff} \quad \mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner),$$

unless $\mathbf{S}$ is fairly *sound* (a term to be defined later). The reason is that the existential quantifier in $\text{Pr}_{\mathbf{T}}$ makes it essentially an ideal statement: While a consistent theory cannot prove false real statements, $\forall x (fx = gx)$, it can prove false existential ones, $\exists x (fx = gx)$. Thus $(*)$ can fail.

The above encoding can be carried out, however, in such a way that the following important conditions are met for all sentences φ ,

$$\text{D1} \quad \mathbf{T} \vdash \varphi \quad \text{implies} \quad \mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner).$$

$$\text{D2} \quad \mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \urcorner).$$

$$\text{D3} \quad \mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \wedge \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \rightarrow \psi \urcorner) \rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \psi \urcorner).$$

Conditions D1–D3 are called the *Derivability Conditions*.

2.2. Proof of the Incompleteness Theorems

The Incompleteness Theorems depend on the following.

2.2.1. THEOREM (Diagonalization Lemma). *Let φx in the language of $\mathbf{T}$ have only the free variable indicated. Then there is a sentence ψ such that*

$$\mathbf{S} \vdash \psi \leftrightarrow \varphi(\ulcorner \psi \urcorner).$$

[N.B. If φ or ψ is not in the language of $\mathbf{S}$, then by “ $\mathbf{S} \vdash \dots$ ”, we mean that the equivalence is proven in the theory $\mathbf{S}'$ in the language of $\mathbf{T}$ whose only non-logical axioms are those of $\mathbf{S}$. $\mathbf{S}'$ is conservative over $\mathbf{S}$.]

PROOF. Given φx , let $\theta x \leftrightarrow \varphi(\text{sub}(x, x))$ be the diagonalization of φ . Let $m = \ulcorner \theta x \urcorner$ and $\psi = \theta m$. Then we claim

$$\mathbf{S} \vdash \psi \leftrightarrow \varphi(\ulcorner \psi \urcorner).$$

For, in $\mathbf{S}$, we see that

$$\begin{aligned} \psi &\leftrightarrow \theta m \leftrightarrow \varphi(\text{sub}(m, m)) \\ &\leftrightarrow \varphi(\text{sub}(\ulcorner \theta x \urcorner, m)) \quad (\text{since } m = \ulcorner \theta x \urcorner) \\ &\leftrightarrow \varphi(\ulcorner \theta m \urcorner) \leftrightarrow \varphi(\ulcorner \psi \urcorner). \quad \square \end{aligned}$$

We apply 2.2.1 to $\neg \text{Pr}_{\mathbf{T}}(x)$.

2.2.2. THEOREM (First Incompleteness Theorem). *Let $\mathbf{T} \vdash \varphi \leftrightarrow \neg \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner)$.*

Then:

- (i) $T \not\vdash \varphi$,
- (ii) *under an additional assumption, $T \not\vdash \neg \varphi$.*

PROOF. (i) Observe $T \vdash \varphi$ implies $T \vdash \text{Pr}_T(\ulcorner \varphi \urcorner)$, by D1, which implies $T \vdash \neg \varphi$, contradicting the consistency of T .

(ii) The additional assumption is a strengthening of the converse to D1, namely $T \vdash \text{Pr}_T(\ulcorner \varphi \urcorner)$ implies $T \vdash \varphi$.

We have $T \vdash \neg \varphi$, hence $T \vdash \neg \neg \text{Pr}_T(\ulcorner \varphi \urcorner)$ so that $T \vdash \text{Pr}_T(\ulcorner \varphi \urcorner)$ and, by the additional assumption, $T \vdash \varphi$, again contradicting the consistency of T . $\square$

2.2.3. THEOREM (Second Incompleteness Theorem). *Let Con_T be $\neg \text{Pr}_T(\ulcorner \Lambda \urcorner)$, where Λ is any convenient contradictory statement. Then*

$$T \not\vdash \text{Con}_T.$$

PROOF. Let φ be as in the statement of Theorem 2.2.2. We show:
 $S \vdash \varphi \leftrightarrow \text{Con}_T$.

Observe that $S \vdash \varphi \rightarrow \neg \text{Pr}_T(\ulcorner \varphi \urcorner)$ implies $S \vdash \varphi \rightarrow \neg \text{Pr}_T(\ulcorner \Lambda \urcorner)$, since $T \vdash \Lambda \rightarrow \varphi$ implies $S \vdash \text{Pr}_T(\ulcorner \Lambda \rightarrow \varphi \urcorner)$, by D1, which implies $S \vdash \text{Pr}_T(\ulcorner \Lambda \urcorner) \rightarrow \text{Pr}_T(\ulcorner \varphi \urcorner)$, by D3.

But $\varphi \rightarrow \neg \text{Pr}_T(\ulcorner \Lambda \urcorner)$ is just $\varphi \rightarrow \text{Con}_T$ and we have proven half of the equivalence.

Conversely, by D2, $S \vdash \text{Pr}_T(\ulcorner \varphi \urcorner) \rightarrow \text{Pr}_T(\ulcorner \text{Pr}_T(\ulcorner \varphi \urcorner) \urcorner)$, which implies $S \vdash \text{Pr}_T(\ulcorner \varphi \urcorner) \rightarrow \text{Pr}_T(\ulcorner \neg \varphi \urcorner)$, by D1, D3, since $\varphi \leftrightarrow \neg \text{Pr}_T(\ulcorner \varphi \urcorner)$. This yields $S \vdash \text{Pr}_T(\ulcorner \varphi \urcorner) \rightarrow \text{Pr}_T(\ulcorner \varphi \wedge \neg \varphi \urcorner)$, by D1, D3, and logic, which implies $S \vdash \text{Pr}_T(\ulcorner \varphi \urcorner) \rightarrow \text{Pr}_T(\ulcorner \Lambda \urcorner)$, by D1, D3, and logic. By contraposition, $S \vdash \neg \text{Pr}_T(\ulcorner \Lambda \urcorner) \rightarrow \neg \text{Pr}_T(\ulcorner \varphi \urcorner)$, which is $S \vdash \text{Con}_T \rightarrow \varphi$, by definitions. $\square$

2.2.4. COROLLARY. $S \vdash \text{Con}_T \rightarrow \text{Con}_{T+\neg \text{Con}_T}$.

PROOF. By the proof of Theorem 2.2.3,

- (i) $S \vdash \text{Con}_T \rightarrow \neg \text{Pr}_T(\ulcorner \varphi \urcorner)$,
- (ii) $S \vdash \text{Con}_T \leftrightarrow \varphi$.

Using D2, D3, it follows that $S \vdash \text{Con}_T \rightarrow \neg \text{Pr}_T(\ulcorner \text{Con}_T \urcorner)$, so that

$$S \vdash \text{Con}_T \rightarrow \neg \text{Pr}_T(\ulcorner \neg \text{Con}_T \rightarrow \Lambda \urcorner),$$

which gives $S \vdash \text{Con}_T \rightarrow \text{Con}_{T+\neg \text{Con}_T}$. $\square$

Corollary 2.2.4 is the Formalized Second Incompleteness Theorem.

Let us finish this exposition of the proofs with two remarks:

2.2.5. REMARK. By the proof of the Second Theorem, the self-referential sentence which asserts its own unprovability is equivalent to the sentence asserting consistency. Hence, this sentence is unique up to provable equivalence and one may correctly speak of *the* sentence that asserts its own unprovability.

2.2.6. REMARK. If the reader compares the loose statement of the First Incompleteness Theorem given earlier with that of Theorem 2.2.2(ii), he will notice that we dropped the reference to ω -consistency. We will discuss this concept in Section 4.2.

2.3. Things to come

Except for the discussion of the mechanics of the encoding, we have finished proving the Incompleteness Theorems. This seems to be a good place to insert a brief description of the sequel.

In Section 3, we discuss the encoding and some related topics. Section 4 concerns metamathematical properties other than consistency and presents some generalizations of the Incompleteness Theorems. In Section 5, we present two applications of the notions and results of Sections 2 and 4. The Incompleteness Theorems are obtained by formalizing Syntax — in Section 6, we discuss what happens when one formalizes Semantics.

3. Encoding

The details of an encoding are fascinating to work out and boring to read. The author wrote the present section for his own benefit and his feelings will not be hurt if the reader chooses to skip it.

In expositions, one often replaces precise statements by imprecise ones, or by precise but false ones. As an example of the latter, it is commonly asserted that one proves the Second Incompleteness Theorem by formalizing the proof of the First. A more correct statement would be that one formalizes D1 by D2 and then reduces the Second Theorem to the First. In Section 2.1, we have been guilty of cheating in two places:

- (i) in our vague formulation of the sense in which **T** contains **S**, and
- (ii) in our remark on sub.

We discuss (i) now and (ii) in 3.2.2.

In Section 2.1 we blithely remarked that **T** contains **S** in the sense that there is the same sort of embedding of **S** into **T** as there is of arithmetic into

set theory. In ordinary mathematical practice, the details of an embedding can be important: Is it continuous? A homomorphism? The same holds here. We must know, e.g., what we mean by $\text{Pr}_T({}^l\text{Pr}_T({}^l\varphi^1)^1)$, where φ is in the language of $\mathbf{T}$ and Pr_T in that of $\mathbf{S}$.

We propose to sweep all of the difficulties under the rug by strengthening the assumption to:

- (i) the language of $\mathbf{S}$ is contained in that of $\mathbf{T}$;
- (ii) the axioms of $\mathbf{S}$ are among those of $\mathbf{T}$.

While (i) and (ii) will make life easy for us in general, they will really grease the wheels when we discuss D2.

The usual cases considered do not satisfy these conditions; but, if one defines $\mathbf{T}'$ to be the conservative extension of $\mathbf{T}$ by the addition of the symbols and axioms of $\mathbf{S}$, one can usually show

$$(*) \quad \mathbf{S} \vdash \forall x [\text{Pr}_T(x) \leftrightarrow \text{Pr}_{T'}(x)],$$

thus reducing the case in question to the one treated here. Theories in which (*) does not hold are pathological and we are not interested in them.

Now that this is settled, we make some additional inessential assumptions. Their only use is to reduce the number of cases that need to be considered when we define various functions representing syntactic operations (cf. 3.2). They are:

- (i) The only logical connectives and quantifiers are $\neg, \rightarrow, \forall$.
- (ii) $\mathbf{S}$ and $\mathbf{T}$ contain as constants only the numerals: $\bar{0}, \bar{1}, \dots$.
- (iii) Only numerical variables occur.
- (iv) $\mathbf{T}$ contains infinitely many n -ary function and relation symbols for each n .

Thus, the language of $\mathbf{T}$ consists of:

numerals: $\bar{0}, \bar{1}, \dots$,

numerical variables: $v_0, v_1, \dots$,

n -ary function symbols: $f_0^n, f_1^n, \dots$,

n -ary relation symbols: $R_0^n, R_1^n, \dots$,

connectives: $\neg, \rightarrow$.

quantifier: $\forall$.

The other connectives and quantifier are considered to be abbreviations.

We assume that $\mathbf{S}$ has a pairing function $\langle \ , \ \rangle$ with inverses π_1, π_2 . Using them, we assign codes, which are closed terms, to the basic syntactic objects as follows:

$$\begin{array}{ll} \bar{i} \mapsto \langle \bar{0}, \bar{i} \rangle & \neg \mapsto \langle \bar{4}, \bar{4} \rangle \\ v_i \mapsto \langle \bar{1}, \bar{i} \rangle & \rightarrow \mapsto \langle \bar{5}, \bar{5} \rangle \end{array}$$

$$f_i^n \mapsto \langle \bar{2}, \langle \bar{n}, \bar{i} \rangle \rangle \quad \forall \mapsto \langle \bar{6}, \bar{6} \rangle$$

$$R_i^n \mapsto \langle \bar{3}, \langle \bar{n}, \bar{i} \rangle \rangle$$

Terms and formulae are finite sequences of these symbols and derivations are finite sequences of formulae. Thus, **S** will have to be able to encode and manipulate finite sequences. In the following subsection, we introduce a nice class of functions and discuss their use for such encoding. In 3.2, we assume these functions are “in” **S** and finish encoding syntax. 3.3, 3.4, and 3.5 discuss some generalizations of the First Incompleteness Theorem that one can prove once one has an awareness of the encoding opportunities available.

3.1. Primitive recursive encoding of finite sequences

Loosely put, the primitive recursive functions are those functions of natural numbers that are obtained by recursion. Of course, to be obtained by recursion, they must be obtained *from* something and, to avoid minor unpleasanties, they must also be closed under explicit definition:

3.1.1. DEFINITION. A function f on natural numbers is *primitive recursive* if it can be generated after finitely many steps by means of the following rules:

- | | | |
|-----|--|-------------|
| i | $f(x) = 0,$ | Zero |
| ii | $f(x) = x + 1,$ | Successor |
| iii | $f(x) = x_i,$ | Projection |
| iv | $f(x) = g(h_1(x), \dots, h_m(x)),$ | Composition |
| v | $\begin{cases} f(0, x) = g(x), \\ f(x+1, x) = h(f(x, x), x, x). \end{cases}$ | Recursion |

3.1.2. DEFINITION. A relation $R \subseteq N^n$ is primitive recursive if its *representing function*,

$$\chi_R(x) = \begin{cases} 0 & \text{if } R(x), \\ 1 & \text{if } \neg R(x) \end{cases}$$

is primitive recursive.

To facilitate the discussion of the encoding of finite sequences, we

establish a few simple closure properties of the classes of primitive recursive functions and relations. To do this, we need a few functions. Trivially, starting with the Zero function and iterating composition of the Successor function, we see that all constant functions are primitive recursive. Elementary school mathematics tells us that iterating Recursion shows that addition, multiplication, and exponentiation are primitive recursive. Subtraction takes us out of the domain of natural numbers; however, *cut-off subtraction*,

$$x \dot{-} y = \begin{cases} x - y & \text{if } x \geq y, \\ 0 & \text{if } x < y, \end{cases}$$

is primitive recursive. For we can define it by Recursion by

$$x \dot{-} 0 = x, \quad x \dot{-} (y + 1) = \text{pd}(x \dot{-} y),$$

where pd is defined by Recursion by

$$\text{pd}(0) = 0, \quad \text{pd}(x + 1) = x.$$

Two more handy functions are the sign function, sg , and its complement, $\overline{\text{sg}}$:

$$\text{sg}(0) = 0, \quad \text{sg}(x + 1) = 1;$$

$$\overline{\text{sg}}(0) = 1, \quad \overline{\text{sg}}(x + 1) = 0.$$

3.1.3. LEMMA (definition by cases). *Let g_1 , g_2 , h be primitive recursive and define f by*

$$f(\mathbf{x}) = \begin{cases} g_1(\mathbf{x}) & \text{if } h(\mathbf{x}) = 0, \\ g_2(\mathbf{x}) & \text{if } h(\mathbf{x}) \neq 0. \end{cases}$$

Then f is primitive recursive.

PROOF. $f(\mathbf{x}) = g_1(\mathbf{x}) \cdot \overline{\text{sg}}(h(\mathbf{x})) + g_2(\mathbf{x}) \cdot \text{sg}(h(\mathbf{x})). \quad \square$

3.1.4. COROLLARY. *The relation of equality is primitive recursive.*

PROOF. Let $h(x, y) = |x - y| = (x \dot{-} y) + (y \dot{-} x). \quad \square$

Note that sg and $\overline{\text{sg}}$ were used in somewhat of a logical manner in the above proof. To further illustrate this, let χ_R , χ_S be the representing functions of relations R , S . Observe:

$$\begin{aligned}\chi_{\neg R}(\mathbf{x}) &= \overline{\text{sg}(\chi_R(\mathbf{x}))}, \\ \chi_{R \wedge S}(\mathbf{x}) &= \text{sg}(\chi_R(\mathbf{x}) + \chi_S(\mathbf{x})), \\ \chi_{R \vee S}(\mathbf{x}) &= \chi_R(\mathbf{x}) \cdot \chi_S(\mathbf{x}).\end{aligned}$$

If we define bounded quantifiers, $\exists y \leq x$, $\forall y \leq x$, then for $R(y, \mathbf{x})$:

$$\chi_{\exists y \leq x R}(\mathbf{x}, \mathbf{x}) = \prod_{y \leq x} \chi_R(y, \mathbf{x}),$$

$$\chi_{\forall y \leq x R} = \chi_{\neg \exists y \leq x \neg R}.$$

3.1.5. LEMMA. (i) *Let $g(x, \mathbf{x})$ be primitive recursive. Then f_1 and f_2 are primitive recursive, where*

$$f_1(x, \mathbf{x}) = \sum_{y \leq x} g(y, \mathbf{x}), \quad f_2(x, \mathbf{x}) = \prod_{y \leq x} g(y, \mathbf{x}).$$

(ii) *If $R(y, \mathbf{x})$ is a primitive recursion relation, then the relations S, T are also primitive recursive, where*

$$S(x, \mathbf{x}) \leftrightarrow \exists y \leq x R(y, \mathbf{x}), \quad T(x, \mathbf{x}) \leftrightarrow \forall y \leq x R(y, \mathbf{x}).$$

The proof of this lemma is left to the reader.

3.1.6. DEFINITION (bounded μ -operator). Let $g(y, \mathbf{x})$ be a function. We define

$$f(x, \mathbf{x}) = \mu y < x [g(y, \mathbf{x}) = 0]$$

by $f(x, \mathbf{x}) =$ the least $y < x$ such that $g(y, \mathbf{x}) = 0$, if such a y exists, and $f(x, \mathbf{x}) = x$, otherwise.

3.1.7. LEMMA. *If $g(y, \mathbf{x})$ is primitive recursive, then so is $\mu y < x [g(y, \mathbf{x}) = 0]$.*

PROOF. Define

$$f_1(x, \mathbf{x}) = \begin{cases} 0 & \text{if } \exists y \leq x [g(y, \mathbf{x}) = 0], \\ 1 & \text{if } \neg \exists y \leq x [g(y, \mathbf{x}) = 0]. \end{cases}$$

f_1 is primitive recursive and we may define

$$f(x, \mathbf{x}) = \sum_{y < x} f_1(y, \mathbf{x}). \quad \square$$

We have enough tools at hand to show the primitive recursiveness of the well-known pairing function,

$$\langle x, y \rangle = \frac{1}{2}((x + y)^2 + 3x + y),$$

and its inverses. We simply use the bounded μ -operator:

$$\langle x, y \rangle = \mu z < (x + y)^2 + 3x + y + 1 [2z = (x + y)^2 + 3x + y],$$

$$\pi_1 z = \mu x < z + 1 [\exists y \leq z (\langle x, y \rangle = z)],$$

$$\pi_2 z = \mu y < z + 1 [\langle \pi_1 z, y \rangle = z],$$

where we use the fact that $x, y \leq \langle x, y \rangle$.

To encode finite sequences, we use the Fundamental Theorem of Arithmetic, whereby every natural number ≥ 2 has a unique representation:

$$a = p_{i_0}^{n_0} \cdots p_{i_k}^{n_k},$$

where $p_{i_0}, \dots, p_{i_k}$ are distinct primes and all n_i are positive. We have the following definitions:

$$\text{i} \quad x \mid y \leftrightarrow \exists z \leq y (xz = y).$$

$$\text{ii} \quad x < y \leftrightarrow \exists z \leq y (y = x + z + 1).$$

$$\text{iii} \quad x \text{ is prime} \leftrightarrow x \neq 0 \wedge x \neq 1 \wedge \forall z \leq x [z \mid x \rightarrow z = x \vee z = 1].$$

$$\text{iv} \quad p_n = n\text{-th prime: } p_0 = 2,$$

$$p_{n+1} = \mu x < p_n! + 1 [p_n < x \wedge x \text{ is prime}].$$

$$\text{v} \quad a \in \text{Seq} \leftrightarrow a = 1 \vee a > 1 \wedge \forall x \leq a [p_{x+1} \mid a \rightarrow p_x \mid a].$$

$$\text{vi} \quad \text{lh}(a) = \begin{cases} 0 & \text{if } a \notin \text{Seq} \vee a = 1, \\ \mu x \leq a [p_x \mid a \wedge p_{x+1} \nmid a] & \text{if } a \in \text{Seq} \wedge a \neq 1. \end{cases}$$

$$\text{vii} \quad (a)_x = \mu y \leq x + 1 [p_x^{y+1} \mid a \wedge p_x^{y+2} \nmid a].$$

$$\text{viii} \quad a * b = \begin{cases} a \cdot \prod_{x \leq \text{lh}(b)} p_{\text{lh}(\bar{a})+x+1}^{(b)_x+1} & \text{if } a \neq 1 \wedge b \neq 1, \\ a & \text{if } b = 1 \wedge a \neq 1, \\ b & \text{if } a = 1. \end{cases}$$

We should comment on v–viii. Seq denotes the set of sequence numbers, i.e. those numbers with no gaps in their list of prime divisors. For such numbers, we have

$$a = \prod_{i \leq \text{lh}(a)} p_i^{(a)_i + 1}.$$

If a, b are sequence numbers encoding $(a_0, \dots, a_m)$, $(b_0, \dots, b_n)$, respectively, then $a * b$ is a sequence number encoding the concatenation $(a_0, \dots, a_m, b_0, \dots, b_n)$.

We write $(a_0, \dots, a_n)$ for $2^{a_0+1} \cdots p_n^{a_n+1}$. In particular, $(a) = 2^{a+1}$ and $() = 1$.

An immediate application of these notions is the following.

3.1.8. LEMMA (course-of-values recursion). *Let g, h be primitive recursive and define f by*

$$f(0, \mathbf{x}) = g(\mathbf{x}), \quad f(x+1, \mathbf{x}) = h(\tilde{f}(x, \mathbf{x}), \mathbf{x}, \mathbf{x}),$$

where $\tilde{f}(x, \mathbf{x}) = (f(0, \mathbf{x}), \dots, f(x, \mathbf{x}))$ is the course-of-values function associated with f . Then f is primitive recursive.

PROOF. Observe that $\tilde{f}$ is primitive recursive:

$$f(0, \mathbf{x}) = 2^{g(\mathbf{x})}, \quad \tilde{f}(x+1, \mathbf{x}) = \tilde{f}(x, \mathbf{x}) * (h(\tilde{f}(x, \mathbf{x}), \mathbf{x}, \mathbf{x})).$$

But $f(x, \mathbf{x}) = (\tilde{f}(x, \mathbf{x}))_x$. $\square$

We will use this lemma in the next subsection to finish our discussion of encoding.

3.2. Primitive recursive encoding of syntax

So far we have codes for basic syntactic objects (variables, numerals, etc.) and a primitive recursive technique of encoding finite sequences. We now combine what we have to encode more complicated syntactic objects.

3.2.1. DEFINITION. We generate codes for complex terms and formulae as follows:

(i) If $t_1, \dots, t_n$ have codes $\ulcorner t_1 \urcorner, \dots, \ulcorner t_n \urcorner$, then

$$\ulcorner f_i^n t_1 \cdots t_n \urcorner = (\ulcorner f_i^n \urcorner, \ulcorner t_1 \urcorner, \dots, \ulcorner t_n \urcorner),$$

$$\ulcorner R_i^n t_1 \cdots t_n \urcorner = (\ulcorner R_i^n \urcorner, \ulcorner t_1 \urcorner, \dots, \ulcorner t_n \urcorner),$$

where $\ulcorner f_i^n \urcorner, \ulcorner R_i^n \urcorner$ are the codes assigned in the introduction.

(ii) If φ, ψ , have codes $\ulcorner \varphi \urcorner, \ulcorner \psi \urcorner$, respectively, then

$$\ulcorner \neg \varphi \urcorner = (\ulcorner \neg \urcorner, \ulcorner \varphi \urcorner), \quad \ulcorner \varphi \rightarrow \psi \urcorner = (\ulcorner \rightarrow \urcorner, \ulcorner \varphi \urcorner, \ulcorner \psi \urcorner).$$

(iii) If φ has code $\ulcorner \varphi \urcorner$ and v_i is a variable, then

$$\ulcorner \forall v_i \varphi \urcorner = (\ulcorner \forall \urcorner, \ulcorner v_i \urcorner, \ulcorner \varphi \urcorner).$$

[Note. This gives us the functions neg, imp: $\text{neg}(x) = (\ulcorner \neg \urcorner, x)$; $\text{imp}(x, y) = (\ulcorner \rightarrow \urcorner, x, y)$.]

We now show that the complex syntactic notions are primitive recursive:

(i) The representing function for terms is defined by course-of-values recursion:

$$T(x) = \begin{cases} 0 & \text{if } \exists i \leq x [x = \langle 0, i \rangle \vee x = \langle 1, i \rangle], \\ 0 & \text{if } x \in \text{Seq} \wedge \exists ni \leq x [(x)_0 = \langle 2, \langle n, i \rangle \rangle \wedge \text{lh}(x) = n \wedge \\ & \wedge \forall y < n (T((x)_{y+1}) = 0)], \\ 1 & \text{otherwise.} \end{cases}$$

(ii) Similarly, one defines the representing function for formulae:

$$F(x) = \begin{cases} 0 & \text{if } x \in \text{Seq} \wedge \exists ni \leq x [(x)_0 = \langle 3, \langle n, i \rangle \rangle \wedge \text{lh}(x) = n \wedge \\ & \wedge \forall y < n (T((x)_{y+1}) = 0)], \\ 0 & \text{if } x \in \text{Seq} \wedge (x)_0 = \ulcorner \neg \urcorner \wedge F((x)_1) = 0 \wedge \text{lh}(x) = 1, \\ 0 & \text{if } x \in \text{Seq} \wedge (x)_0 = \ulcorner \rightarrow \urcorner \wedge F((x)_1) = F((x)_2) = 0 \wedge \text{lh}(x) = 2, \\ 0 & \text{if } x \in \text{Seq} \wedge (x)_0 = \ulcorner \forall \urcorner \wedge \exists i \leq x ((x)_1 = \langle 1, i \rangle) \\ & \wedge F((x)_2) = 0 \wedge \text{lh}(x) = 2, \\ 1 & \text{otherwise.} \end{cases}$$

3.2.2. Sub

In Section 2.1 we spoke of a substitution function. As it is, we need two: one to replace a (code for a) free variable by a (code for a) term and one to replace a (code for a) free variable by a (code for a) numeral which supposedly designates the same number designated by a given term. The former is needed, e.g., to recognize axioms such as $\forall x \varphi x \rightarrow \varphi t$. Both could be used for the Diagonalization Lemma; but the latter is needed if one wants a free-variable form of the Diagonalization Lemma. Other uses are hard to describe here and we leave the function to “speak for itself” when we apply it later. We define the first syntactic substitution function by course-of-values recursion, first treating terms and then formulae:

$$\begin{aligned}
\text{sub}(\ulcorner v_i \urcorner, i, y) &= y, \\
\text{sub}(\ulcorner v_j \urcorner, i, y) &= \ulcorner v_j \urcorner, \quad j \neq i, \\
\text{sub}(\ulcorner f_j^n t_1 \cdots t_n \urcorner, i, y) &= (\ulcorner f_j^n \urcorner, \text{sub}(\ulcorner t_1 \urcorner, i, y), \dots, \text{sub}(\ulcorner t_n \urcorner, i, y)), \\
\text{sub}(\ulcorner R_j^n t_1 \cdots t_n \urcorner, i, y) &= (\ulcorner R_j^n \urcorner, \text{sub}(\ulcorner t_1 \urcorner, i, y), \dots, \text{sub}(\ulcorner t_n \urcorner, i, y)), \\
\text{sub}(\ulcorner \neg \varphi \urcorner, i, y) &= (\ulcorner \neg \urcorner, \text{sub}(\ulcorner \varphi \urcorner, i, y)), \\
\text{sub}(\ulcorner \varphi \rightarrow \psi \urcorner, i, y) &= (\ulcorner \rightarrow \urcorner, \text{sub}(\ulcorner \varphi \urcorner, i, y), \text{sub}(\ulcorner \psi \urcorner, i, y)), \\
\text{sub}(\ulcorner \forall v, \varphi \urcorner, i, y) &= \ulcorner \forall v, \varphi \urcorner, \\
\text{sub}(\ulcorner \forall v_j \varphi \urcorner, i, y) &= (\ulcorner \forall \urcorner, \ulcorner v_j \urcorner, \text{sub}(\ulcorner \varphi \urcorner, i, y)), \\
\text{sub}(x, i, y) &= 0, \quad x \text{ not of the above forms.}
\end{aligned}$$

With this definition, one easily sees that, for any term t ,

$$\text{sub}(\ulcorner \varphi v_i \urcorner, i, \ulcorner t \urcorner) = \ulcorner \varphi t \urcorner.$$

If we observe that v_i occurs freely in φ iff $\text{sub}(\ulcorner \varphi \urcorner, i, \langle 0, i \rangle) \neq \ulcorner \varphi \urcorner$, then we can primitive recursively define the function sub referred to in Section 2.1 by

$$\text{sub}(x, y) = \begin{cases} \text{sub}(x, i, y) & \text{if } i = \mu j < x [v_j \text{ occurs free in } x], \\ x & \text{if } i \text{ does not exist.} \end{cases}$$

$\text{sub}_3, \text{sub}_4$, etc. are defined by iteration.

A second important substitution function is

$$s(x, y) = \text{sub}(x, \langle 0, y \rangle).$$

This satisfies: If φv_i has only v_i free, t is a closed term denoting n , then $s(\ulcorner \varphi v_i \urcorner, t) = \ulcorner \psi \urcorner$, where ψ is equivalent to $\varphi \bar{n}$. (To prove $\psi \leftrightarrow \varphi \bar{n}$, one need only show $\vdash t = \bar{n}$. For then, substitutivity of equality yields $\vdash \ulcorner \varphi \bar{n} \urcorner = \ulcorner \psi \urcorner$.) Moreover, if φ has only v_i free, $s(\ulcorner \varphi \urcorner, x)$ is formally the code of a sentence. We often abbreviate $s(\ulcorner \varphi x \urcorner, y)$ by $\ulcorner \varphi y \urcorner$.

3.2.3. Prov_T

The next step is to define $\text{Prov}_T(x, y)$. A derivation of φ is a sequence of formulae such that each element of the sequence is either an axiom of T , a logical axiom, or a consequence by some logical rule of earlier members of the sequence. The logical axioms can be taken to be primitive recursive in the sense that the set of codes of such axioms is primitive recursive. We leave it to the reader to check this for his favorite axiomatization. Further,

by clever choice of axioms, we can assume that the only rule of inference is modus ponens:

$$\text{MP: } \frac{\varphi \quad \varphi \rightarrow \psi}{\psi}.$$

We assume that the set of (codes of) axioms of **T** is primitive recursive. Thus, we get:

$$\begin{aligned} \text{Prov}_T(x, y) \leftrightarrow & x \in \text{Seq} \wedge \forall i \leq \text{lh}(x) [(x)_i \text{ is a logical axiom} \vee \\ & \vee (x)_i \text{ is an axiom of } T \vee \\ & \vee \exists jk < i ((x)_k = \text{imp}((x)_j, (x)_i))] \wedge \\ & \wedge y = (x)_{\text{lh}(x)}. \\ \text{Pr}_T(y) \leftrightarrow & \exists x \text{ Prov}_T(x, y). \end{aligned}$$

3.2.4. **S, I: Numeralwise representability**

A relation $R \subseteq N^n$ is said to be *numeralwise represented* or *numerated* by a formula φ in **S** if one has, for all $m_1 \cdots m_n$,

$$Rm_1 \cdots m_n \text{ is true} \quad \text{iff} \quad \mathbf{S} \vdash \varphi \bar{m}_1 \cdots \bar{m}_n.$$

R is *binumerated* by φ if one also has

$$Rm_1 \cdots m_n \text{ is false} \quad \text{iff} \quad \mathbf{S} \vdash \neg \varphi \bar{m}_1 \cdots \bar{m}_n.$$

We assume that **S** binumerates every primitive recursive relation. To do this, it suffices to find a formula φ_f for every primitive recursion function f , such that all numerical instances of the defining equations for f are provable. E.g. if f is defined by Recursion from g, h , then for all $m_1, \dots, m_n, m$,

$$\begin{aligned} \mathbf{S} \vdash & \exists! x \varphi_f(\bar{0}, \bar{m}_1, \dots, \bar{m}_n, x) \wedge \forall x [\varphi_f(\bar{0}, \bar{m}_1, \dots, \bar{m}_n, x) \rightarrow \varphi_g(\bar{m}_1, \dots, \bar{m}_n, x)], \\ \mathbf{S} \vdash & \exists! x \varphi_f(\bar{m} + \bar{1}, \bar{m}_1, \dots, \bar{m}_n, x) \\ & \wedge \forall x, y [\varphi_f(\bar{m}, \bar{m}_1, \dots, \bar{m}_n, y) \wedge \\ & \wedge \varphi_f(\bar{m} + \bar{1}, \bar{m}_1, \dots, \bar{m}_n, x) \rightarrow \varphi_h(y, \bar{m}, \bar{m}_1, \dots, \bar{m}_n, x)]. \end{aligned}$$

Then, a metamathematical induction on the number of steps it takes to generate f (and on the first argument of f in the case of definition by recursion) shows that φ_f binumerates the graph of f .

Given that **S** binumerates all primitive recursive functions (and hence all primitive recursive relations), it follows that all of the primitive recursive

encoding functions are binumerated: neg, imp, sub, s, and Prov_T . This last fact allows us to verify D1:

$$\begin{aligned} T \vdash \varphi &\Leftrightarrow S \vdash \text{Prov}_T(t, \ulcorner \varphi \urcorner) \quad \text{for some closed term } t, \\ &\Rightarrow S \vdash \text{Pr}_T(\ulcorner \varphi \urcorner). \end{aligned}$$

A quick rereading of the proof of the First Incompleteness Theorem will show that we did not need D2 and D3 to establish it. Thus we have given (modulo only a little handwaving) a complete proof of this Theorem.

3.2.5. S, II: D2 and D3

The Second Incompleteness Theorem does not come so cheaply. For D3, one must show

$$S \vdash \text{Prov}_T(a, \ulcorner \varphi \urcorner) \wedge \text{Prov}_T(b, \ulcorner \varphi \rightarrow \psi \urcorner) \rightarrow \text{Prov}_T(a * b * (\ulcorner \psi \urcorner), \ulcorner \psi \urcorner),$$

with *free* variables a, b . To do this requires much more than mere binumerability of primitive recursive relations: The representations must be correct with free variables. For this, S must be able to prove not merely each instance of the defining equations for a given primitive recursive function, but must also prove the equations with free variables. It will also be necessary for S to prove induction on primitive recursive relations.

The latter necessity is clear if one considers D2. D2 is a formal version of the following sharpening of D1: If f is primitive recursive,

$$\begin{aligned} (*) \quad fm_1 \cdots m_n = m &\Rightarrow T \vdash f\bar{m}_1 \cdots \bar{m}_n = \bar{m} \\ &\Rightarrow S \vdash \text{Prov}_T(d(\bar{m}_1, \dots, \bar{m}_n), \ulcorner f\bar{m}_1 \cdots \bar{m}_n = \bar{m} \urcorner), \end{aligned}$$

for some primitive recursive function d . To see that such a d exists, observe that a proof that $fm = m$ (in S , and hence in T) is almost just a computation — it will be given by a sequence of equations and implications of equations. Thus, the existence of d satisfying $(*)$ is not too surprising; nor is the fact that we claim:

$$(**) \quad S \vdash fx = y \rightarrow \text{Prov}_T(dx, \ulcorner f\bar{x} = \bar{y} \urcorner).$$

The proof, which is too long to be included here, proceeds by metamathematical induction on the number of steps needed to generate f and (when the recursion clause is used) formal induction on the primitive recursive relation $(**)$. Once one has accepted $(**)$, the primitive recursiveness of Prov_T yields

$$S \vdash \text{Prov}_T(x, y) \rightarrow \text{Pr}_T(\ulcorner \text{Prov}_T(\bar{x}, \bar{y}) \urcorner),$$

and one needs only apply D1, D3 to the valid formula $\varphi x \rightarrow \exists x \varphi x$, to conclude the validity of D2.

3.2.6. S, III: Choice of S

By the preceding discussion, one can adequately encode syntax in **S** if **S** admits a representation of primitive recursive functions in such a way that

(i) the defining equations for primitive recursive functions are provable with free variables;

(ii) induction on primitive recursive relations is provable;

(iii) computations are almost derivations of the equations they establish.

We list three examples of such theories.

(a) **PRA** = Primitive Recursive Arithmetic. **PRA** contains the numerals $\bar{0}, \bar{1}, \dots$ and there is a function symbol in **PRA** for each (definition via the rules for the generation of primitive recursive functions of a) primitive recursive function. In addition to some trivial axioms concerning the constants and the successor function, the axioms of **PRA** are the defining equations of the functions and induction on quantifier-free formulae.

(b) **PA** = Peano's Arithmetic. **PA** also has the numerals as its constants, but it only has function symbols for successor, addition, and multiplication. The axioms consist of trivial axioms concerning the constants and the successor function, the recursion equations for addition and multiplication, and induction on all formulae of the language. Even proving that **PA** binumerates the primitive recursive functions requires another encoding trick. The most famous technique uses the Chinese Remainder Theorem to encode finite sequences. Conditions (i) and (ii) are proven by formalizing the use of the encoding of finite sequences and is non-trivial insofar as very few texts give the details. Condition (iii) can be bypassed by observing that the representation of a PR function can be written in the form $\exists x \varphi$, where φ is much simpler syntactically than the corresponding primitive recursive function. E.g., by Matiyasevich's Theorem, φ can be taken to be an equation involving two polynomials. Thus, the formalization of $\varphi x \rightarrow \text{Pr}_{\text{PA}}(\ulcorner \varphi x \urcorner)$ is much simpler.

(c) **ZF** = Zermelo–Fraenkel set theory. This is both a good and a bad example. It is bad because the whole encoding problem is more easily solved in a set theory than in an arithmetic theory. By the same token, it is a good example.

3.3. Rosser's Theorem

By Section 3.2, binumerability of primitive recursive relations in **S**

suffices for the First Incompleteness Theorem — as a condition on **S**. There is still the necessity of assuming something about **T** —

- (i) that **T** contain **S**,
- (ii) that **T** be consistent, and
- (iii) (for the second half of the theorem) that theorems of **T** of the form $\text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner)$ be true.

Rosser's Theorem allows one to drop the last soundness condition on **T** by using a modification of $\text{Prov}_{\mathbf{T}}$: Define

$$\begin{aligned}\text{Prov}_{\mathbf{T}}^R(x, y) &\leftrightarrow \text{Prov}_{\mathbf{T}}(x, y) \wedge \\ &\wedge \forall zw \leq x [\text{Prov}_{\mathbf{T}}(z, w) \rightarrow y \neq \text{neg}(w) \wedge w \neq \text{neg}(y)], \\ \text{Pr}_{\mathbf{T}}^R(y) &\leftrightarrow \exists x \text{Prov}_{\mathbf{T}}^R(x, y), \\ \text{Con}_{\mathbf{T}}^R &\leftrightarrow \neg \text{Pr}_{\mathbf{T}}^R(\ulcorner \Lambda \urcorner).\end{aligned}$$

3.3.1. ROSSER'S THEOREM. *Let $\mathbf{T} \vdash \varphi \leftrightarrow \neg \text{Pr}_{\mathbf{T}}^R(\ulcorner \varphi \urcorner)$. Then*

- (i) $\mathbf{T} \not\vdash \varphi$;
- (ii) $\mathbf{T} \not\vdash \neg \varphi$;
- (iii) $\mathbf{T} \vdash \text{Con}_{\mathbf{T}}^R$.

PROOF. (i) By the consistency of **T**, $\text{Prov}_{\mathbf{T}}$ and $\text{Prov}_{\mathbf{T}}^R$ binumerate the same relation. Hence D1^R holds: $\mathbf{T} \vdash \psi \Rightarrow \vdash \text{Pr}_{\mathbf{T}}^R(\ulcorner \psi \urcorner)$. Thus, the proof of the first part of the First Incompleteness Theorem yields the result.

(ii) This follows from (iii).

(iii) We leave this to the reader along with the remark that **T** is consistent and $\mathbf{T} \vdash \neg \Lambda$. $\square$

*3.4. Recursion theory

(The reader is referred to Chapter C.1 for a full discussion of recursion theory.)

Historically, recursion theory developed out of the incompleteness theorems. Once one knows a little recursion theory, however, it is natural to look back.

3.4.1. DEFINITION. A set $\mathbf{S} \subseteq \mathbb{N}$ of natural numbers is *recursively enumerable* (r.e.) iff for some primitive recursive relation R ,

$$\mathbf{S}x \Leftrightarrow \exists y Rxy.$$

An equivalent definition is:

3.4.2. DEFINITION. A set $S \subseteq \mathbb{N}$ is r.e. iff $S = \emptyset$ or, for some primitive recursive function f , $S = \text{ran}(f)$.

Another useful concept is given by the following definition.

3.4.3. DEFINITION. A set $S \subseteq \mathbb{N}$ is *recursive* iff S and $\mathbb{N} - S$ are both r.e. A function $f: \mathbb{N} \rightarrow \mathbb{N}$ is recursive iff its graph (viewed as a subset of $\mathbb{N}$ by means of a primitive recursive pairing function) is recursive.

The recursion-theoretic counterpart of the First Incompleteness Theorem is:

3.4.4. THEOREM. *There is an r.e. non-recursive set.*

One proves this by finding an enumeration, $W_0, W_1, \dots$, of r.e. sets and an r.e. set K_1 such that

$$\forall xy (\langle x, y \rangle \in K_1 \Leftrightarrow x \in W_y).$$

Then $K = \{x: \langle x, x \rangle \in K_1\}$ is r.e. with a non-r.e. complement. One then proves the First Incompleteness Theorem by showing that K can be numeralwise represented in T . If T is sound enough, this is not too difficult — one uses the numeralwise representation of K in S that arises from the binumeration of the primitive recursive relation that K is the projection of. If T is not very sound, the numeralwise representation of K in S may not be one in T as T may simply prove more numbers to be in K . One usually avoids difficulties with numeralwise representations in unsound theories by means of the following:

3.4.5. DEFINITION. Let $A, B \subseteq \mathbb{N}$ be disjoint r.e. sets. A and B are *effectively inseparable* iff there is a recursive function f such that for all r.e. sets W_i, W_j , if

$$(i) \quad W_i \cap W_j = \emptyset,$$

$$(ii) \quad A \subseteq W_i, \quad B \subseteq W_j,$$

then $f(i, j) \notin W_i \cup W_j$.

3.4.6. THEOREM. *Effectively inseparable r.e. sets exist.*

We shall accept this on faith.

To prove that part of Rosser's Theorem that corresponds to the First Incompleteness Theorem, one constructs φ, ψ which numeralwise represent A, B , respectively, in S and for which

$$(*) \quad \mathbf{S} \vdash \forall x \neg (\varphi x \wedge \psi x).$$

Then, if $\mathbf{T}$ is a consistent formal theory, the set of (codes of) its theorems can be shown to be r.e. and one defines

$$W_i = \{n: \mathbf{T} \vdash \varphi \bar{n}\}, \quad W_j = \{n: \mathbf{T} \vdash \neg \varphi \bar{n}\}.$$

By (*), $W_i \cap W_j = \emptyset$. Since $\mathbf{T}$ contains $\mathbf{S}$ and φ numerates A in $\mathbf{S}$, it follows that $A \subseteq W_i$, $B \subseteq W_j$ and $n_0 = f(i, j) \notin W_i \cup W_j$. Thus $\mathbf{T} \not\vdash \varphi \bar{n}_0, \neg \varphi \bar{n}_0$.

*3.5. The formula hierarchy

The purpose of the present subsection is mainly to establish some notation for several more advanced sections below.

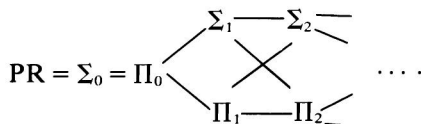
Recall that $\mathbf{S}$ is assumed to have, for each primitive recursive function f , a formula φ_f representing it in the strong sense of 3.2.5. φ_f is called a *primitive recursive formula*, or a PR formula.

3.5.1. DEFINITION. A formula φ is Σ_n (Π_n) iff for some PR formula ψ ,

$$\varphi = Q_1 x_1 \cdots Q_n x_n \psi,$$

where $Q_1 = \exists$ ($\forall$) and the quantifiers alternate in type. We write $\varphi \in \Sigma_n$ (Π_n), ambiguously, as φ is Σ_n (Π_n) or provably equivalent (in $\mathbf{S}$) to a Σ_n (Π_n) formula.

Thus, one has the inclusions:



3.5.2. THEOREM. *There is a Σ_n truth definition for Σ_n formulae. I.e., for each n , there is a formula $\text{Tr}_{\Sigma_n} \in \Sigma_n$ with only the numerical variable x free such that, for $\varphi_x \in \Sigma_n$,*

$$\mathbf{S} \vdash \varphi x \leftrightarrow \text{Tr}_{\Sigma_n}({}^1\varphi \dot{x}^1).$$

A similar result holds for Π_n .

We omit the proof and note the following.

3.5.3. COROLLARY. *The formula $\text{Tr}_{\Sigma_n}(s(x, x))$ is Σ_n , non- Π_n .*

The proof is left as an easy exercise to the reader.

It follows that all the inclusions indicated above are proper. Thus we have a genuine hierarchy.

From our point of view, there are two uses of this Hierarchy: First, since it is a hierarchy, we can use it to measure the complexity of formulae or of sets of formulae. Such use is made in Section 4. A second use is not of the Hierarchy itself taken as a hierarchy, but rather of Theorem 3.5.2: Many set-theoretic proofs could be carried out in arithmetic *if* one had a truth definition. Tarski's Theorem asserts that there is no truth definition for the entire language [Exercise]. By Theorem 3.5.2, there are partial truth definitions $\text{Tr}_0, \text{Tr}_1, \dots$ such that Tr_n works up to the n -th level of the Hierarchy. This allows the formalization of certain outwardly set-theoretic constructions within arithmetic. An application is discussed in Section 6.

Before proceeding, it is worth noting the following.

3.5.4. FACT (demonstrable Σ_1 completeness). *If $\varphi \in \Sigma_1$, then*

$$\mathbf{S} \vdash \varphi \mathbf{x} \rightarrow \text{Pr}_T(\ulcorner \varphi \mathbf{x} \urcorner).$$

This follows from the discussion of 3.2.5.

4. Metamathematical properties other than consistency

Metamathematically, consistency is a minimal assumption on a theory. One might wish for stronger properties to hold — e.g. ω -consistency. If $\mathbf{T}$ is a theory about a particular structure, as PA is a theory about the semiring of natural numbers, one might wish for even more — *soundness* (anything provable is true) or *completeness* (anything or its negation is provable — hence anything true is provable).

In this section, we discuss these properties. In 4.1 we consider a soundness scheme — the *Reflection Principle*. ω -consistency is discussed in 4.2 and its relation to the more intuitive Reflection Principle is presented. Completeness, which we know to be false, nonetheless gives rise to consistent schemata. These are discussed in 4.3.

4.1. Reflection principles

The First Incompleteness Theorem is proven by considering the sentence that asserts its own *unprovability*. Under minimal assumptions, it is clear that the sentence must be true — and hence unprovable. But what about the sentence that asserts its own *provability*? Is it true? false? It was precisely this problem that led to the following important theorem characterizing provable instances of the Reflection Principle:

4.1.1. LÖB'S THEOREM. *Let φ be closed. Then*

$$\mathbf{T} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi \quad \text{iff} \quad \mathbf{T} \vdash \varphi.$$

PROOF. The one direction is obvious. For the other, assume that $\mathbf{T} \not\vdash \varphi$. Then $\mathbf{T} + \neg \varphi$ is consistent and we may appeal to the Second Incompleteness Theorem to conclude that $\mathbf{T} + \neg \varphi$ does not yield $\text{Con}_{\mathbf{T} + \neg \varphi}$, hence not $\neg \text{Pr}_{\mathbf{T}}(\ulcorner \neg \varphi \rightarrow \Lambda \urcorner)$. Thus

$$\mathbf{T} + \neg \varphi \not\vdash \neg \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner).$$

Contraposition yields $\mathbf{T} \not\vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi$. $\square$

As hinted above, this solves the problem of sentences asserting their own provability — such sentences are provable (and hence equivalent — cf. also 5.1). This also focuses our attention on the following schemata:

Local Reflection Principle

$$\text{Rfn}(\mathbf{T}): \quad \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi, \quad \varphi \text{ closed.}$$

First Uniform Reflection Principle

$$\text{RFN}(\mathbf{T}): \quad \forall x \text{ Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \urcorner) \rightarrow \forall x \varphi x, \quad \varphi \text{ has only } x \text{ free.}$$

Second Uniform Reflection Principle

$$\text{RFN}'(\mathbf{T}): \quad \forall x [\text{Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \urcorner) \rightarrow \varphi x], \quad \varphi \text{ has only } x \text{ free.}$$

[A stipulation must be inserted here: As indicated by the notation $\ulcorner \varphi \dot{x} \urcorner$, the variable x must range over elements which can be named by constants. Thus, we insist that the x in the uniform versions of the Reflection Principle be a numerical variable. In fact, throughout the following, we shall assume that all variables explicitly exhibited are numerical variables, although non-numerical variables may occur unexhibited in the formulae.]

The reflection principles are clearly schematic assertions of soundness — anything provable is true. As such, they immediately imply consistency and, thus, we see that they are underivable in $\mathbf{T}$. Of course, Theorem 4.1.1 tells us more than this: It characterizes the provable instances of $\text{Rfn}(\mathbf{T})$. Nonetheless, it may be instructive to restate the First and Second Incompleteness Theorems in terms of the reflection principles:

4.1.2. FIRST INCOMPLETENESS THEOREM. *For some true, unprovable φ ,*

$$\mathbf{T} \not\vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi.$$

4.1.3. SECOND INCOMPLETENESS THEOREM. *For any refutable φ ,*

$$\mathbf{T} \not\vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi.$$

Let us check that these statements are equivalent to the more familiar versions. The First Incompleteness Theorem is no problem if we specify that the true unprovable sentence we have in mind is the one asserting its own unprovability. Then Theorem 4.1.1 simply yields

$$\mathbf{T} \not\vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi \quad \text{iff} \quad \mathbf{T} \not\vdash \varphi,$$

where the two equivalents are the two versions of the First Incompleteness Theorem. For the Second Incompleteness Theorem, observe that, for refutable φ , the following are equivalent over $\mathbf{T}$:

$$\text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi \quad \neg \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \quad \neg \text{Pr}_{\mathbf{T}}(\ulcorner \Delta \urcorner) \quad \text{Con}_{\mathbf{T}}.$$

Theorem 4.1.1 again yields the equivalence of the two versions.

Thus, Löb's Theorem is a generalization of the incompleteness theorems. While this alone would justify taking a closer look at the reflection principles, it might be worth our while to mention another motivating factor. Recall that the main impetus behind Hilbert's Consistency Program was the fact that consistency was equivalent to soundness for real statements:

4.1.4. THEOREM. *Over $\mathbf{S}$, the following are equivalent:*

- (i) $\text{Con}_{\mathbf{T}}$;
- (ii) $\text{Rfn}_{\Pi_1}(\mathbf{T})$;
- (iii) $\text{RFN}_{\Pi_1}(\mathbf{T})$;
- (iv) $\text{RFN}'_{\Pi_1}(\mathbf{T})$;

where the subscript " Π_1 " indicates restriction of the schemata to $\varphi \in \Pi_1$.

PROOF. The implications (iv) $\rightarrow$ (iii) $\rightarrow$ (ii) are fairly direct. (ii) $\rightarrow$ (i) follows from the above observation that $\text{Con}_{\mathbf{T}} \leftrightarrow (\text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi)$ for any refutable φ — one merely chooses such a $\varphi \in \Pi_1$.

(i) $\rightarrow$ (iv). Let $\varphi \in \Pi_1$ have only x free. Then $\neg \varphi x \in \Sigma_1$ and, by demonstrable Σ_1 -completeness (see 3.5),

$$(*) \quad \mathbf{S} \vdash \neg \varphi x \rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \neg \varphi x \urcorner).$$

But

$$(**) \quad \mathbf{S} + \text{Con}_{\mathbf{T}} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi x \urcorner) \rightarrow \neg \text{Pr}_{\mathbf{T}}(\ulcorner \neg \varphi x \urcorner),$$

whence (*) and (**) combine to give

$$\mathbf{S} + \text{Con}_{\mathbf{T}} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi x \urcorner) \rightarrow \varphi x. \quad \square$$

The interested reader is referred to 5.2 for some applications of Theorem 4.1.4. For the moment, we simply use it as our second reason to justify our interest in reflection principles: *Consistency is equivalent to a restricted Reflection Principle*.

Having decided that reflection principles are worth studying, we may as well begin. First, let us observe that the schemata are listed in full generality. For one thing, we must restrict ourselves to schemata since the sentence

$$\forall x [\text{Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \urcorner) \rightarrow \text{Tr}(\ulcorner \varphi \dot{x} \urcorner)],$$

where $\text{Tr}(\ulcorner \psi \urcorner)$ asserts “ ψ is true”, cannot be asserted in $\mathbf{T}$. For, by Tarski’s Theorem on Truth Definitions, there can be no truth definition for $\mathbf{T}$ within $\mathbf{T}$ itself (cf. 3.5). Further, extra variables in either version of the uniform scheme can be contracted by means of a pairing function, reducing the general scheme to the two listed. A hybrid, e.g. $\forall x [\forall y \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \dot{y} \urcorner) \rightarrow \forall y \varphi xy]$, is clearly implied by the several variable Second Uniform Reflection Principle. Finally, we have the following theorem.

4.1.5. THEOREM (Feferman). *RFN($\mathbf{T}$) and RFN’($\mathbf{T}$) are equivalent over $\mathbf{S}$.*

PROOF. Obviously, the instance, $\forall x \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \urcorner) \rightarrow \forall x \varphi x$, of RFN($\mathbf{T}$) is implied by the corresponding instance of RFN’($\mathbf{T}$). The converse requires a minor (but often useful) lemma:

4.1.6. LEMMA. $\mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \text{Prov}_{\mathbf{T}}(\dot{y}, \ulcorner \varphi \dot{x} \urcorner) \urcorner) \rightarrow \varphi \dot{x}$.

PROOF. (a) By D1 and D3,

$$\begin{aligned} \mathbf{S} \vdash \text{Prov}_{\mathbf{T}}(y, \ulcorner \varphi \dot{x} \urcorner) &\rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \urcorner) \\ &\rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \text{Prov}_{\mathbf{T}}(\dot{y}, \ulcorner \varphi \dot{x} \urcorner) \urcorner) \rightarrow \varphi \dot{x}. \end{aligned}$$

(b) Since $\neg \text{Prov}_{\mathbf{T}} \in \text{PR}$, we similarly have

$$\begin{aligned} \mathbf{S} \vdash \neg \text{Prov}_{\mathbf{T}}(y, \ulcorner \varphi \dot{x} \urcorner) &\rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \neg \text{Prov}_{\mathbf{T}}(\dot{y}, \ulcorner \varphi \dot{x} \urcorner) \urcorner) \\ &\rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \text{Prov}_{\mathbf{T}}(\dot{y}, \ulcorner \varphi \dot{x} \urcorner) \urcorner) \rightarrow \varphi \dot{x}. \end{aligned}$$

Combining (a) and (b) yields the lemma. $\square$

To complete the proof of Theorem 4.1.5, let φ be given and observe

$$\mathbf{S} \vdash \forall x [\text{Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \urcorner) \rightarrow \varphi x] \leftrightarrow \forall xy [\text{Prov}_{\mathbf{T}}(y, \ulcorner \varphi \dot{x} \urcorner) \rightarrow \varphi x].$$

But the right-hand side of this equivalence is derivable in $\mathbf{S} + \mathbf{RFN}(\mathbf{T})$ by Lemma 4.1.6. $\square$

Before proceeding further, it is amusing to note the following provable instance of reflection:

$$(*) \quad \mathbf{S} \vdash \exists y \text{Pr}_{\mathbf{T}}(\ulcorner \text{Prov}_{\mathbf{T}}(y, \ulcorner \varphi \urcorner) \urcorner) \rightarrow \exists y \text{Prov}_{\mathbf{T}}(y, \ulcorner \varphi \urcorner),$$

i.e. $\mathbf{S} \vdash \exists y \text{Pr}_{\mathbf{T}}(\ulcorner \text{Prov}_{\mathbf{T}}(y, \ulcorner \varphi \urcorner) \urcorner) \rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner)$. (*) follows immediately from Lemma 4.1.6 and condition D3 and we leave its derivation to the reader. By Theorem 4.1.4 and the Second Incompleteness Theorem, the variable y on the right side of (*) cannot in general denote the same code for a derivation as the y on the left. We can also see this by appeal to the following free-variable form of Löb's Theorem:

4.1.7. THEOREM. *Let φ have only x free. Then*

$$\mathbf{T} \vdash \forall x \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \urcorner) \rightarrow \varphi x \quad \text{iff} \quad \mathbf{T} \vdash \forall x \varphi x.$$

We omit the proof.

So far, we have shown that the use of reflection principles allows a generalization of the incompleteness theorems, that $\text{Con}_{\mathbf{T}}$ is equivalent to a restriction of the Reflection schemata, and that $\mathbf{RFN}(\mathbf{T})$ is as general as $\mathbf{RFN}'(\mathbf{T})$ and further schemata with additional variables. We ought to ask ourselves the simple question: How much of an improvement is Reflection over Consistency? Obviously, consistency does not imply soundness — e.g. $\mathbf{T} = \mathbf{PA} + \neg \text{Con}_{\mathbf{PA}}$ is consistent but not sound as $\neg \text{Con}_{\mathbf{PA}}$ is a false theorem of $\mathbf{T}$. (For this same $\mathbf{T}$, however, $\mathbf{T} + \text{Con}_{\mathbf{T}} \vdash \mathbf{RFN}(\mathbf{T})$ — for $\mathbf{T} \vdash \neg \text{Con}_{\mathbf{T}}$.) A first step is given by the following simple lemma:

4.1.8. LEMMA. *Let φ be closed. Then*

- (i) $\mathbf{T} + \varphi + \mathbf{Rfn}(\mathbf{T}) \vdash \mathbf{Rfn}(\mathbf{T} + \varphi)$,
- (ii) $\mathbf{T} + \varphi + \mathbf{RFN}(\mathbf{T}) \vdash \mathbf{RFN}(\mathbf{T} + \varphi)$.

PROOF. Observe that for any ψ , we have the following over $\mathbf{S}$:

$$\mathbf{S} \vdash \text{Pr}_{\mathbf{T}+\varphi}(\ulcorner \psi \urcorner) \leftrightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \rightarrow \psi \urcorner). \quad \square$$

4.1.9. COROLLARY. *Let φ be closed.*

- (i) *Let $\mathbf{T} + \varphi$ be consistent. Then $\mathbf{T} + \varphi \not\vdash \mathbf{Rfn}(\mathbf{T})$.*
- (ii) *Let $\mathbf{T}'$ be a consistent finite extension of $\mathbf{T}$. Then $\mathbf{T}' \not\vdash \mathbf{Rfn}(\mathbf{T})$.*
- (iii) *If $\mathbf{T} + \text{Con}_{\mathbf{T}}$ is consistent, then $\mathbf{T} + \text{Con}_{\mathbf{T}} \not\vdash \mathbf{Rfn}(\mathbf{T})$.*

*4.1^a. Hierarchy considerations

By Corollary 4.1.9, neither $\text{Rfn}(\mathbf{T})$ nor $\text{RFN}(\mathbf{T})$ is implied by any finite set of axioms consistent with $\mathbf{T}$. We devote the rest of this subsection to discussing an often useful improvement of this in the uniform case. For this purpose, we must use the notions and notations of the Formula Hierarchy (discussed in 3.5). This material is less detailed and may be omitted on first reading.

Let $\text{RFN}_{\Pi_k}(\mathbf{T})$ denote the restriction of the scheme $\text{RFN}(\mathbf{T})$ to formulae in Π_k . Similarly, one defines $\text{RFN}_{\Sigma_k}(\mathbf{T})$, $\text{RFN}'_{\Pi_k}(\mathbf{T})$, and $\text{RFN}'_{\Sigma_k}(\mathbf{T})$. A first result is:

4.1.10. THEOREM. *Over $\mathbf{S}$, the following are equivalent ($k \geq 0$):*

- (i) $\text{RFN}_{\Sigma_k}(\mathbf{T})$,
- (ii) $\text{RFN}_{\Pi_{k+1}}(\mathbf{T})$,
- (i.a) $\text{RFN}'_{\Sigma_k}(\mathbf{T})$,
- (ii.a) $\text{RFN}'_{\Pi_{k+1}}(\mathbf{T})$.

The equivalences $(x) \leftrightarrow (x.a)$ follow by taking a closer look at the proof of Theorem 4.1.5. The implications $(ii) \rightarrow (i)$, $(ii.a) \rightarrow (i.a)$ are trivial as $\Sigma_k \subseteq \Pi_{k+1}$. For the converses, one uses provable closure under numerical substitution: $\mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \forall x \varphi x \urcorner) \rightarrow \forall x \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \dot{x} \urcorner)$.

In terms of the Hierarchy, Lemma 4.1.8 can be restated:

4.1.11. THEOREM. *Let $\varphi \in \Pi_k$ be closed and let $n \geq k$. Then*

- (i) $\mathbf{S} + \varphi + \text{Rfn}_{\Sigma_n}(\mathbf{T}) \vdash \text{Rfn}_{\Sigma_n}(\mathbf{T} + \varphi)$,
- (ii) $\mathbf{S} + \varphi + \text{RFN}_{\Sigma_n}(\mathbf{T}) \vdash \text{RFN}_{\Sigma_n}(\mathbf{T} + \varphi)$.

This is seen by observing that, if $\psi \in \Sigma_n$, then $\varphi \rightarrow \psi \in \Sigma_n$.

Using a Π_k truth definition for Π_k formulae, it can be shown that $\text{RFN}'_{\Pi_k}(\mathbf{T})$ can be written as a single Π_k sentence. Bearing this in mind, we have:

4.1.12. COROLLARY. (i) $\mathbf{T} + \text{RFN}_{\Sigma_{k+1}}(\mathbf{T}) \vdash \text{RFN}_{\Sigma_{k+1}}(\mathbf{T} + \text{RFN}_{\Pi_{k+1}}(\mathbf{T}))$, $k \geq 0$.

(ii) $\mathbf{T} + \text{RFN}_{\Pi_{k+1}}(\mathbf{T}) \vdash \text{RFN}_{\Pi_{k+1}}(\mathbf{T} + \text{RFN}_{\Pi_k}(\mathbf{T}))$, $k \geq 1$.

(iii) *If $\mathbf{T} + \text{RFN}_{\Pi_k}(\mathbf{T})$ is consistent, then*

$$\mathbf{T} + \text{RFN}_{\Pi_k}(\mathbf{T}) \not\vdash \text{Rfn}_{\Sigma_k}(\mathbf{T}), \quad k \geq 1.$$

(iii') *If $\mathbf{T} + \text{Con}_{\mathbf{T}}$ is consistent, then*

$$\mathbf{T} + \text{Con}_{\mathbf{T}} \not\vdash \text{Rfn}_{\Sigma_1}(\mathbf{T}).$$

PROOF. Parts (i) and (ii) follow from Theorems 4.1.10 and 4.1.11. Parts (iii) and (iii') are simple applications of the incompleteness theorems in the forms of Theorems 4.1.2 and 4.1.3. $\square$

By Corollary 4.1.12, RFN is not implied by any (consistent) bounded set of its instances. The following theorem of Kreisel and Levy improves this immensely:

4.1.13. ESSENTIAL UNBOUNDEDNESS THEOREM. *Let n be given. Let $\mathbf{U}$ be an r.e. theory (not necessarily containing $\mathbf{S}$) in the language of $\mathbf{T}$. If $\mathbf{T} \vdash \text{RFN}(\mathbf{U})$, then no consistent extension of $\mathbf{U}$ by a set Δ of Σ_n sentences implies all theorems of $\mathbf{T}$. In particular, $\mathbf{T}$ cannot be axiomatized over $\mathbf{U}$ by any set of Σ_n axioms.*

PROOF. Let Tr_n be a Σ_n truth definition for Σ_n formulae. Define ψ by

$$\mathbf{S} \vdash \psi \leftrightarrow \forall x [\text{Tr}_n(x) \rightarrow \neg \text{Pr}_{\mathbf{U}}(\text{imp}(x, \ulcorner \psi \urcorner))].$$

Intuitively, ψ asserts its unprovability from any true Σ_n sentence.

(a) Since $\mathbf{T} \vdash \text{RFN}(\mathbf{U})$, it follows that

$$\mathbf{T} \vdash \forall x [\text{Pr}_{\mathbf{U}}(\text{imp}(x, \ulcorner \psi \urcorner)) \rightarrow (\text{Tr}_n(x) \rightarrow \psi)].$$

Thus

$$\begin{aligned} \mathbf{T} \vdash \neg \psi &\rightarrow \forall x [\neg \text{Tr}_n(x) \vee \neg \text{Pr}_{\mathbf{U}}(\text{imp}(x, \ulcorner \psi \urcorner))] \\ &\rightarrow \forall x [\text{Tr}_n(x) \rightarrow \neg \text{Pr}_{\mathbf{U}}(\text{imp}(x, \ulcorner \psi \urcorner))] \rightarrow \psi. \end{aligned}$$

Thus $\mathbf{T} \vdash \psi$.

(b) Suppose $\mathbf{U} + \Delta$ extends $\mathbf{T}$; $\Delta \subseteq \Sigma_n$. Then $\mathbf{U} + \Delta \vdash \psi$. We now show that this implies the inconsistency of $\mathbf{U} + \Delta$: Since $\mathbf{U} + \Delta \vdash \psi$, it follows that $\mathbf{U} + X \vdash \psi$ for some finite $X \subseteq \Delta$. Let $\varphi = \bigwedge X$. Then $\mathbf{U} \vdash \varphi \rightarrow \psi$. But this implies

$$(i) \quad \mathbf{T} \vdash \text{Pr}_{\mathbf{U}}(\ulcorner \varphi \rightarrow \psi \urcorner).$$

Since $\mathbf{T} \vdash \psi$,

$$(ii) \quad \mathbf{T} \vdash \text{Pr}_{\mathbf{U}}(\ulcorner \varphi \rightarrow \psi \urcorner) \rightarrow \neg \text{Tr}_n(\ulcorner \varphi \urcorner).$$

But $\varphi \in \Sigma_n$ and

$$(iii) \quad \mathbf{T} \vdash \varphi \leftrightarrow \text{Tr}_n(\ulcorner \varphi \urcorner),$$

and (i)–(iii) yield $\mathbf{T} \vdash \neg \varphi$. $\square$

The Essential Unboundedness Theorem is a useful tool for proving unboundedness theorems — results of the form: Axiomatizing T_1 over T_2 requires arbitrarily complicated formulae. The most basic example is that in which $T_2 = PC$:

4.1.14. DEFINITION. T is said to be *reflexive* if $T \vdash \text{RFN}(PC)$, where PC denotes the predicate calculus (as formulated in the language of T).

We remark that, by Lemma 4.1.8, if T is reflexive, $T \vdash \text{RFN}(U)$ for all finite subsystems U of T . In particular, $T \vdash \text{Con}_U$ for such U .

4.1.15. REFLEXIVENESS THEOREM. *PA and ZF are reflexive.*

The usual proof of this theorem is too long to be given here. For ZF, we can give the following simple proof: By formalized induction on the length of a derivation,

$$\mathbf{ZF} \vdash \forall x [\text{Pr}_{\mathbf{PC}}(\ulcorner \varphi \dot{x} \urcorner) \rightarrow \forall a (\text{Trans}(a) \wedge x \in a \rightarrow \varphi^{(a)}x)],$$

where $\varphi^{(a)}$ denotes the relativization of φ to a and $\text{Trans}(a)$ asserts that a is transitive. By the set-theoretic reflection principle,

$$\mathbf{ZF} \vdash \forall x [\neg \varphi x \rightarrow \exists a [\text{Trans}(a) \wedge x \in a \wedge \neg \varphi^{(a)}x]],$$

whence

$$\mathbf{ZF} \vdash \forall x [\text{Pr}_{\mathbf{PC}}(\ulcorner \varphi \dot{x} \urcorner) \rightarrow \varphi x].$$

As corollaries, we see that (i) the induction scheme of **PA** is not implied by any bounded set of its instances, and (ii) one cannot bound all the schemata of **ZF**.

*4.2. ω -consistency

The concept of ω -consistency was introduced by Gödel for the purpose of stating the hypotheses needed for the First Incompleteness Theorem. The ω -consistency of T is neither the optimal nor the most intuitive condition sufficient for the theorem. Nonetheless, its use here is so firmly entrenched in the literature that we are obligated to comment on it.

Informally, ω -consistency is the property that holds of T if the following two conditions are *not* simultaneously satisfied for any φ :

- (i) $T \vdash \exists x \varphi x$;
- (ii) $T \vdash \neg \varphi \bar{0}, \neg \varphi \bar{1}, \dots$

Formally, ω -consistency can be represented (in varying degrees of generality) by (modifications of) the following scheme:

4.2.1.

$$\text{Pr}_T(\ulcorner \exists x \varphi x \urcorner) \rightarrow \exists x \neg \text{Pr}_T(\ulcorner \neg \varphi x \urcorner).$$

Let 1-Con_T denote the restriction of 4.2.1 to $\varphi \in \text{PR}$ possessing only one free variable.

4.2.2. FORMALIZED FIRST INCOMPLETENESS THEOREM. *Let φ be $\neg \text{Pr}_T(\ulcorner \varphi \urcorner)$. Then:*

- (i) $\mathbf{T} + \text{Con}_T \vdash \neg \text{Pr}_T(\ulcorner \varphi \urcorner)$,
- (ii) $\mathbf{T} + 1\text{-Con}_T \vdash \neg \text{Pr}_T(\ulcorner \neg \varphi \urcorner)$.

PROOF. Part (i) was shown in the course of the proof of the Second Incompleteness Theorem.

For part (ii), let $\varphi = \forall x \psi x$, $\psi \in \text{PR}$. Then

$$\mathbf{T} + 1\text{-Con}_T \vdash \text{Pr}_T(\ulcorner \neg \varphi \urcorner) \rightarrow \exists x \neg \text{Pr}_T(\ulcorner \psi x \urcorner) \rightarrow \exists x \neg \psi x,$$

by demonstrable Σ_1 -completeness (3.5.4). Thus,

$$(*) \quad \mathbf{T} + 1\text{-Con}_T \vdash \text{Pr}_T(\ulcorner \neg \varphi \urcorner) \rightarrow \neg \varphi$$

$$(**) \quad \rightarrow \text{Pr}_T(\ulcorner \varphi \urcorner).$$

But 1-Con_T yields Con_T since it asserts the unprovability of something. Thus, by (i),

$$\mathbf{T} + 1\text{-Con}_T \vdash \neg \text{Pr}_T(\ulcorner \varphi \urcorner),$$

which, with (**), yields (ii). $\square$

Probably the most important thing to notice about the above proof is that 1-Con_T was used only to derive (*): $\text{Pr}_T(\ulcorner \neg \varphi \urcorner) \rightarrow \neg \varphi$, for closed $\varphi \in \Pi_1$ — i.e., 1-Con_T was used only to derive $\text{Rfn}_{\Sigma_1}(\mathbf{T})$. Conversely, $\text{Rfn}_{\Sigma_1}(\mathbf{T})$ can be used to derive 1-Con_T :

$$\begin{aligned} \mathbf{S} + \text{Rfn}_{\Sigma_1}(\mathbf{T}) \vdash \text{Pr}_T(\ulcorner \exists x \varphi x \urcorner) &\rightarrow \exists x \varphi_x \\ &\rightarrow \exists x \neg \text{Pr}_T(\ulcorner \neg \varphi x \urcorner), \end{aligned}$$

since $\neg \varphi x \leftrightarrow \text{Pr}_T(\ulcorner \neg \varphi x \urcorner)$ by demonstrable PR-completeness and the fact that $\text{Rfn}_{\Sigma_1}(\mathbf{T})$ implies Con_T .

By the preceding paragraph, $\text{Rfn}_{\Sigma_1}(\mathbf{T})$ and 1-Con_T are equivalent. Since the statement 4.2.1 of ω -consistency is easily seen to be Σ_2 , Corollary 4.1.12 shows that we cannot expect such behavior to hold for more than some very special cases.

4.2.3. DEFINITION. We define the following formal schemata representing ω -consistency:

Local ω -consistency

$\omega\text{-CON}_T: \quad \text{Pr}_T(\ulcorner \exists x \varphi x \urcorner) \rightarrow \exists x \neg \text{Pr}_T(\ulcorner \neg \varphi \dot{x} \urcorner), \quad \varphi \text{ has only } x \text{ free,}$

Uniform ω -consistency

$\omega\text{-CON}_T: \forall y [\text{Pr}_T(\ulcorner \exists x \varphi x y \urcorner) \rightarrow \exists x \neg \text{Pr}_T(\ulcorner \neg \varphi \dot{x} y \urcorner)], \quad \varphi \text{ has only } x, y \text{ free,}$

Global ω -consistency

$\omega\text{-CON}_T^G: \quad \forall \varphi [\text{Pr}_T(\ulcorner \exists x \varphi x \urcorner) \rightarrow \exists x \neg \text{Pr}_T(\ulcorner \neg \varphi \dot{x} \urcorner)],$

where $\forall \varphi$ indicates quantification over codes of formulae possessing only one free variable.

We hasten to emphasize the fact that, unlike the case with reflection principles, we have here a *global* representation of the given concept as well as the local and uniform ones. The reason is simply that we only use φ in 4.2.1 in the form of a *code* and not, as with reflection, as a subformula of some larger formula. Thus, we can quantify over all φ in the present context.

It is not hard to see that $\omega\text{-CON}_T^G \vdash \omega\text{-CON}_T \vdash \omega\text{-Con}_T$ over **S**. Local schemata are usually difficult to deal with and so we ignore $\omega\text{-Con}_T$. Thus, we are interested in $\omega\text{-CON}_T^G$ and $\omega\text{-CON}_T$ — and in their hierarchical restrictions:

4.2.4. DEFINITION. Let $k \geq 1$. The restriction of $\omega\text{-CON}_T$ to formulae $\varphi \in \Sigma_{k-1}$ is termed $k\text{-CON}_T$ and the corresponding informal concept is called *k-consistency*.

Observe that, via a Σ_k truth definition for Σ_k formulae, the corresponding restriction of $\omega\text{-CON}_T^G$ ($\forall \varphi \mapsto \forall \varphi \in \Sigma_k$) is equivalent to $(k+1)\text{-CON}_T$. Further, as in Theorem 4.1.10, $k\text{-CON}_T$ is equivalent to the corresponding restriction for $\varphi \in \Pi_k$.

The following theorem characterizes these notions in terms of the more intuitive reflection principles:

4.2.5. THEOREM. *Over **S**, we have*

- i $k\text{-CON}_T \leftrightarrow \text{RFN}_{\Pi_{k+1}}(\mathbf{T}), \quad (k = 1, 2)$
- ii $k\text{-CON}_T \leftrightarrow \text{RFN}_{\Pi_3}(\mathbf{T} + \text{RFN}_{\Pi_k}(\mathbf{T})), \quad (k \geq 2)$

$$\text{iii} \quad \omega\text{-CON}_T^G \leftrightarrow \text{RFN}_{\Pi_3}(T + \text{RFN}(T)),$$

$$\text{iii}' \quad \omega\text{-CON}_T^G \leftrightarrow \text{RFN}_{\Pi_3}(T + \omega\text{-CON}_T).$$

The proof is rather long and we omit it. Some related results are covered in Chapter D.2.

[As an aside, we would like to mention the following: The formula hierarchy can, as an obvious use, be applied to obtain quantitative refinements of various results. See e.g. 4.1^a. Theorem 4.2.5 gives an application of a different order: The explication of ω -consistency as a Reflection Principle (iii) presupposes an understanding of the expression " Π_3 ". I.e. one must know something about the formula hierarchy even to state the relation between ω -consistency and soundness.]

4.3. Completeness properties

Somewhat loosely, the First Incompleteness Theorem asserts that consistent strong formal theories are incomplete. Nonetheless, there are consistent schemata asserting completeness. We (need) consider only the local versions:

Syntactic completeness

$$\text{SynComp}_T: \quad \text{Pr}_T(\ulcorner \varphi \urcorner) \vee \text{Pr}_T(\ulcorner \neg \varphi \urcorner), \quad \text{closed } \varphi.$$

Semantic completeness

$$\text{SemComp}_T: \quad \varphi \rightarrow \text{Pr}_T(\ulcorner \varphi \urcorner), \quad \text{closed } \varphi.$$

ω -completeness

$$\omega\text{-Comp}_T: \quad \forall x \text{ Pr}_T(\ulcorner \varphi x \urcorner) \rightarrow \text{Pr}_T(\ulcorner \forall x \varphi x \urcorner), \quad \varphi \text{ has only } x \text{ free.}$$

Without further ado, we state:

4.3.1. THEOREM. *The following are equivalent over S:*

- (i) $\neg \text{Con}_T$;
- (ii) SynComp_T ;
- (iii) SemComp_T ;
- (iv) $\omega\text{-Comp}_T$.

PROOF. Obviously (i) $\rightarrow$ (ii), (iii), (iv).

(ii) $\rightarrow$ (i) We appeal to a Formalized Rosser's Theorem: If φ is $\neg \text{Pr}_T^R(\ulcorner \varphi \urcorner)$, then

$$S + \text{Con}_T \vdash \neg \text{Pr}_T(\ulcorner \varphi \urcorner), \quad \neg \text{Pr}_T(\ulcorner \neg \varphi \urcorner),$$

whence

$$\mathbf{S} + \text{SynComp}_T \vdash \neg \text{Con}_T.$$

(iii) $\rightarrow$ (i) Here, one takes $\varphi = \text{Con}_T$ and applies the Second Incompleteness Theorem. We omit the details in favor of the following case:

(iv) $\rightarrow$ (i) Let $\varphi x = \neg \text{Prov}_T(x, \ulcorner \Lambda \urcorner)$. By Lemma 4.1.6,

$$\mathbf{S} \vdash \forall x \text{Pr}_T(\ulcorner \neg \text{Prov}_T(x, \ulcorner \Lambda \urcorner) \urcorner),$$

whence

$$\mathbf{S} + \omega\text{-Comp}_T \vdash \text{Pr}_T(\ulcorner \forall x \neg \text{Prov}_T(x, \ulcorner \Lambda \urcorner) \urcorner)$$

$$\vdash \text{Pr}_T(\ulcorner \text{Pr}_T(\ulcorner \Lambda \urcorner) \rightarrow \Lambda \urcorner)$$

$$\vdash \text{Pr}_T(\ulcorner \Lambda \urcorner),$$

by the Formalized Löb's Theorem: $\mathbf{S} \vdash \text{Pr}_T(\ulcorner \text{Pr}_T(\ulcorner \varphi \urcorner) \rightarrow \varphi \urcorner) \rightarrow \text{Pr}_T(\ulcorner \varphi \urcorner)$. $\square$

*4.3^a. Kent's Theorem

By Theorem 4.3.1(iii), the scheme $\varphi \rightarrow \text{Pr}_T(\ulcorner \varphi \urcorner)$, is equivalent to $\neg \text{Con}_T$ and, hence, is not in general derivable — not even when restricted to $\varphi \in \Pi_1$ (namely $\varphi = \text{Con}_T$). We also know, from 3.5.4, that the subscheme $\varphi x \rightarrow \text{Pr}_T(\ulcorner \varphi x \urcorner)$, $\varphi \in \Sigma_1$, is derivable. The following Theorem of Kent shows that the situation is even more complicated yet:

4.3.2. THEOREM. *For any n , there is a sentence φ such that*

(i) $\mathbf{S} \vdash \varphi \rightarrow \text{Pr}_S(\ulcorner \varphi \urcorner)$;

(ii) *For no $\psi \in \Sigma_n$ does $\mathbf{S} \vdash \varphi \leftrightarrow \psi$.*

PROOF. First, let χ be such that for *no* $\psi \in \Sigma_n$ consistent with $\mathbf{S}$ do we have

$$(*) \quad \mathbf{S} + \psi \vdash \chi \quad \text{or} \quad \mathbf{S} + \psi \vdash \neg \chi.$$

To construct such a χ , we take a hint from the Essential Unboundedness Theorem and let

$$\chi \leftrightarrow \forall x [\text{Tr}_n(x) \rightarrow \neg \text{Pr}_S^R(\text{imp}(x, \ulcorner \chi \urcorner))],$$

where Tr_n is a Σ_n truth definition for Σ_n formulae. Mimicking the proof of Rosser's Theorem, we see that (*) fails for all $\psi \in \Sigma_n$ consistent with $\mathbf{S}$.

Now let φ be $\chi \wedge \text{Pr}_S(\ulcorner \Lambda \urcorner)$. Clearly (i) holds. To see (ii), suppose $\mathbf{S} \vdash \varphi \leftrightarrow \psi$ for $\psi \in \Sigma_n$. Then $\mathbf{S} \vdash \psi \rightarrow \varphi$, so $\mathbf{S} \vdash \neg \psi$, since otherwise (*) is true. Since $\neg \varphi$ is $\neg (\chi \wedge \text{Pr}_S(\ulcorner \Lambda \urcorner))$, $\mathbf{S} \vdash \neg \varphi$, so $\mathbf{S} \vdash \text{Pr}_S(\ulcorner \Lambda \urcorner) \rightarrow \neg \chi$, contradicting $\neg (*)$ since $\mathbf{S} + \text{Pr}_S(\ulcorner \Lambda \urcorner)$ is consistent. $\square$

5. Two applications

5.1. A fix-point theorem

By diagonalization, one easily finds sentences ψ , χ such that

$$\mathbf{S} \vdash \psi \leftrightarrow \neg \text{Pr}_{\mathbf{T}}(\ulcorner \psi \urcorner), \quad \mathbf{S} \vdash \chi \leftrightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \chi \urcorner).$$

The proof of the Second Incompleteness Theorem and Löb's Theorem, respectively, yielded the interesting facts that ψ and χ were not only unique, but explicitly definable:

$$\mathbf{S} \vdash \psi \leftrightarrow \text{Con}_{\mathbf{T}} \leftrightarrow \neg \text{Pr}_{\mathbf{T}}(\ulcorner \Delta \urcorner),$$

$$\mathbf{S} \vdash \chi \leftrightarrow \mathbf{t},$$

where $\mathbf{t}$ = truth. An older proof of Löb's Theorem uses the fix-point,

$$\theta \leftrightarrow (\text{Pr}_{\mathbf{T}}(\ulcorner \theta \urcorner) \rightarrow \varphi),$$

for any given φ . A little algebra soon reveals

$$\theta \leftrightarrow (\text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \varphi),$$

whence θ too is explicitly definable — this time from the remaining variable. These turn out not to be isolated examples, but rather instances of a general result.

To obtain a simple statement of this result, we consider a propositional language with propositional variables $p, q, r, \dots$; the usual connectives, $\wedge, \vee, \neg, \rightarrow$; propositional constants $\mathbf{t}, \mathbf{f}$ for truth and falsity; and a modal operator $\Box$ to stand for provability. This will be an interpreted system rather than a deductive one: Given an assignment, $p \mapsto \varphi_p$, of sentences to propositional variables, we obtain a translation φ_α for each formula α of the propositional language:

$$\varphi_{\alpha \circ \beta} = \varphi_\alpha \circ \varphi_\beta, \quad \circ = \wedge, \vee, \rightarrow;$$

$$\varphi_{\neg \alpha} = \neg \varphi_\alpha; \quad \varphi_{\Box \alpha} = \text{Pr}_{\mathbf{T}}(\ulcorner \varphi_\alpha \urcorner).$$

If $\alpha(p_1, \dots, p_n)$ is a formula of the propositional language and we assign ψ_i to p_i , then we write $\alpha(\psi_1, \dots, \psi_n)$ for $\varphi_{\alpha(p_1, \dots, p_n)}$, i.e. for the result of substituting each ψ_i for the corresponding p_i and $\text{Pr}_{\mathbf{T}}$ for $\Box$.

5.1.1. THEOREM (De Jongh's Fix-Point Theorem¹). *Let $\alpha(p, q)$ be such that p occurs only inside the scope of $\Box$. Then, for some $\beta(q)$ and all sentences $\psi_1, \dots, \psi_n$ of the language of $\mathbf{T}$,*

¹ A proof of Theorem 5.1.1 has now been published in SAMBIN [0000].

$$S \vdash \beta(\psi) \leftrightarrow \alpha(\beta(\psi), \psi).$$

Further, $\beta(\psi)$ is, up to provable equivalence, the only fix-point of α .

The proof of this is too complicated to be included here. However, we can prove the following special case:

5.1.2. THEOREM. *Let $\alpha(p, q) = \alpha'(\Box \gamma(p, q), q)$, where in $\alpha'(x, y)$ the variable x does not occur inside the scope of a $\Box$. Then the fix-points of α are determined parametrically by*

$$\beta(q) = \alpha'[\Box \gamma(\alpha'(t, q), q), q].$$

PROOF. Although we are interested in establishing the result with sentences ψ replacing the variables q , the propositional notation is more convenient. An expression $\vdash \delta(q) \leftrightarrow \delta'(q)$ is understood accordingly.

Since the Diagonalization Lemma holds, we may assume that we have a p such that $\vdash p \leftrightarrow \alpha(p, q)$. It will follow from this that $\vdash p \leftrightarrow \beta(q)$.

5.1.3. LEMMA. *For all r, t, δ , $r \leftrightarrow t$, $\Box(r \leftrightarrow t) \vdash \delta(r) \leftrightarrow \delta(t)$.*

This follows from the derivability conditions by induction on the length of δ . We omit the proof.

To prove Theorem 5.1.2, we first show:

$$(*) \quad \vdash \Box \gamma(p, q) \leftrightarrow \Box \gamma(\alpha'(t, q), q).$$

By the fix-point assumption, $\vdash p \leftrightarrow \alpha'(\Box \gamma(p, q), q)$. Thus, since $\Box \gamma(p, q)$ does not occur inside the scope of $\Box$ in α' ,

$$(**) \quad \Box \gamma(p, q) \vdash \Box \gamma(p, q) \leftrightarrow t \\ \vdash \alpha'(\Box \gamma, q) \leftrightarrow \alpha'(t, q) \vdash p \leftrightarrow \alpha'(t, q).$$

The derivability conditions yield

$$(***) \quad \Box \gamma(p, q) \vdash \Box \Box \gamma(p, q) \vdash \Box(p \leftrightarrow \alpha'(t, q)).$$

Applying the lemma to (**), (***), we immediately have

$$\Box \gamma(p, q) \vdash \Box \gamma(\alpha'(t, q), q),$$

i.e. half of (*).

For the converse, assume $\Box \gamma(p, q) \wedge \neg \gamma(p, q)$. Then

$$\Box \gamma(p, q) \wedge \neg \gamma(p, q) \vdash \neg \gamma(\alpha'(t, q), q),$$

by the same reasoning as above. Contraposition yields

$$\gamma(\alpha'(\mathbf{t}, q), q) \vdash \Box \gamma(p, q) \rightarrow \gamma(p, q),$$

whence

$$\Box \gamma(\alpha'(\mathbf{t}, q), q) \rightarrow \Box(\Box \gamma(p, q) \rightarrow \gamma(p, q)) \rightarrow \Box \gamma(p, q),$$

by the Formalized Löb's Theorem,

$$\mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \urcorner \rightarrow \ulcorner \varphi \urcorner) \rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner).$$

This completes the proof of (*).

To conclude the proof, observe

$$\beta(q) = \alpha'[\Box \gamma(\alpha'(\mathbf{t}, q), q), q] \leftrightarrow \alpha'(\Box \gamma(p, q), q) \text{ by } (*)$$

$$\leftrightarrow p,$$

the latter by choice of p . $\square$

5.1.4. EXAMPLE. We list: (i) $\alpha(p, q)$, (ii) $\alpha'(p, q)$, (iii) $\gamma(p, q)$, (iv) $\Box \gamma(\alpha'(\mathbf{t}, q), q)$, (v) $\beta(q)$, and (vi) a final simplification of (v):

	(a)	(b)	(c)	(d)
(i)	$\neg \Box p$	$\Box p$	$\Box p \rightarrow q$	$\Box(p \rightarrow q)$
(ii)	$\neg p$	p	$p \rightarrow q$	p
(iii)	p	p	p	$p \rightarrow q$
(iv)	$\Box \neg \mathbf{t}$	$\Box \mathbf{t}$	$\Box(\mathbf{t} \rightarrow q)$	$\Box(\mathbf{t} \rightarrow q)$
(v)	$\neg \Box \neg \mathbf{t}$	$\Box \mathbf{t}$	$\Box(\mathbf{t} \rightarrow q) \rightarrow q$	$\Box(\mathbf{t} \rightarrow q)$
(vi)	$\neg \Box \mathbf{f}$	$\mathbf{t}$	$\Box q \rightarrow q$	$\Box q$

5.2. Conservation results

In this section, we present some conservation results of Kreisel.

Recall that Hilbert's Conservation Program called for a proof that the use of ideal statements and abstract reasoning led to no new real theorems. While the incompleteness theorems showed that this is *in general* impossible, they do not rule out the possibility of success in special cases. In fact, we will even use the Second Incompleteness Theorem in establishing one conservation result

First, we present the main result:

5.2.1. CONSERVATION THEOREM. *Let $\varphi \in \Pi_1$. Then $\mathbf{T} \vdash \varphi \Rightarrow \mathbf{S} + \text{Con}_{\mathbf{T}} \vdash \varphi$.*

PROOF. Let $\varphi \in \Pi_1$ and suppose $\mathbf{T} \vdash \varphi$. D1 yields $\mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner)$. But $\text{Con}_{\mathbf{T}}$ is equivalent to $\text{RFN}_{\Pi_1}(\mathbf{T})$ over $\mathbf{S}$ by Theorem 4.1.4, whence $\mathbf{S} + \text{Con}_{\mathbf{T}} \vdash \varphi$. $\square$

The next two results are corollaries:

5.2.2. THEOREM. *Let $\varphi \in \Pi_1$. Then $\mathbf{T} + \neg \text{Con}_{\mathbf{T}} \vdash \varphi \Rightarrow \mathbf{T} \vdash \varphi$.*

PROOF.

$$\begin{aligned} \mathbf{T} + \neg \text{Con}_{\mathbf{T}} \vdash \varphi &\Rightarrow \mathbf{T} + \text{Con}_{\mathbf{T} + \neg \text{Con}_{\mathbf{T}}} \vdash \varphi, \quad \text{by Theorem 5.2.1} \\ &\Rightarrow \mathbf{T} + \text{Con}_{\mathbf{T}} \vdash \varphi, \end{aligned}$$

by the Formalized Second Incompleteness Theorem. But we have

$$\mathbf{T} + \text{Con}_{\mathbf{T}} \vdash \varphi, \quad \mathbf{T} + \neg \text{Con}_{\mathbf{T}} \vdash \varphi,$$

whence $\mathbf{T} \vdash \varphi$. $\square$

5.2.3. THEOREM. *Let $\mathbf{T}, \mathbf{T}'$ contain $\mathbf{S}$ and let*

$$(*) \quad \mathbf{T} \vdash \forall x [\text{Prov}_{\mathbf{T}'}(x, \ulcorner \varphi \urcorner) \rightarrow \text{Prov}_{\mathbf{T}}(tx, \ulcorner \psi \urcorner)]$$

for some primitive recursive term t . Then $\mathbf{S} \vdash \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner) \rightarrow \text{Pr}_{\mathbf{T}}(\ulcorner \psi \urcorner)$.

PROOF. By the Conservation Theorem,

$$\mathbf{S} + \text{Con}_{\mathbf{T}} \vdash (*) \vdash \neg \text{Pr}_{\mathbf{T}}(\ulcorner \psi \urcorner) \rightarrow \neg \text{Pr}_{\mathbf{T}}(\ulcorner \varphi \urcorner),$$

by contraposition. Now absorb $\text{Con}_{\mathbf{T}}$ into $\neg \text{Pr}_{\mathbf{T}}(\ulcorner \psi \urcorner)$ and contrapose again. $\square$

5.2.4. COROLLARY (Relative Consistency Theorem). *Let $\mathbf{T}, \mathbf{T}'$ contain $\mathbf{S}$ and let*

$$\mathbf{S} \vdash \forall x [\text{Prov}_{\mathbf{T}'}(x, \ulcorner \Lambda \urcorner) \rightarrow \text{Prov}_{\mathbf{T}}(tx, \ulcorner \Lambda \urcorner)]$$

for some primitive recursive term t . Then $\mathbf{S} \vdash \text{Con}_{\mathbf{T}} \rightarrow \text{Con}_{\mathbf{T}'}$.

The corollary is worth commenting on. By the Second Incompleteness Theorem, one cannot prove consistency of strong theories within weak theories. Sometimes, the consistency of a strong theory is genuinely in doubt and one can give a relative consistency result, e.g.

$$(**) \quad \text{Con}_{\mathbf{ZF}} \rightarrow \text{Con}_{\mathbf{ZF} + \neg \text{CH}}.$$

A throwback to Hilbert's Consistency Program is the demand that the proof of (**) be carried out within as weak a system as possible. Epistemologically, there is no need to give a proof of (**) in, say, **PA**: For, the value of (**) depends entirely on the acceptance of ZF and one might as

well prove (**) in the latter theory — a technically easier undertaking. However, we can avoid philosophical bickering; for, by Corollary 5.2.4, if this is done at all nicely, it automatically follows that (**) can be proven in the weaker theory — namely **PRA**. Thus, there is nothing to argue about here.

In the last paragraph, we pointed out how one conservation result caused a potential philosophical problem to vanish. Usually, the value of conservation results is that they allow one to use stronger techniques to shorten proofs and conserve one's energy. We refer the reader to Chapter D.3 for quantitative information.

*6. The formalized completeness theorem

There are several possible advanced topics that one could discuss. The close relation between induction principles and reflection principles (often bearing the misnomer, “consistency proofs”) is discussed in Chapter D.2. One could discuss efforts to complete a formally incomplete theory by the iterated addition of reflection principles. Another topic concerns proof-theoretic applications of the reflection principles.

We shall discuss the formalized completeness theorem and use it to give model-theoretic proofs of the incompleteness theorems.

In this section, we set $S = \mathbf{PA}$.

*6.1. The Hilbert–Bernays Completeness Theorem

Formalizing the Henkin completeness proof within **PA** yields:

6.1.1. HILBERT–BERNAYS COMPLETENESS THEOREM. *Let U have a primitive recursive set of axioms. There is a Δ_2 set of formulae, Tr_M , such that in $\mathbf{PA} + \text{Con}_U$ one can prove that this set defines a model of U :*

$$\mathbf{PA} + \text{Con}_U \vdash \forall x (\text{Pr}_U(x) \rightarrow \text{Tr}_M(x)).$$

Let us explain this: A formula φ is said to be Δ_n if it can be written both as a Σ_n and a Π_n formula. Theorem 6.1.1 asserts that, modulo Con_U , one can prove in **PA** the existence of a model of U whose truth definition is Δ_2 .

The meaning of this is best understood by a description of the proof, which is just an arithmetization of the set-theoretic one: One adds to the language of U an infinite primitive recursive set of new constants $c_0, c_1, \dots$, and adds the axiom

$$(*) \quad \exists x \varphi x \rightarrow \varphi(c_{[\varphi]})$$

for each formula φ . One then enumerates all sentences $\varphi_0, \varphi_1, \dots$ of this augmented language and defines a complete theory by starting with **U** and adding, at step n , φ_n or $\neg \varphi_n$ — according to whether φ_n is consistent with what has been chosen before or not. The construction is readily described within **PA**. Assuming $\text{Con}_{\mathbf{U}}$, one can also prove that the construction never terminates. The resulting set of sentences forms a complete theory which, by virtue of the axioms $(*)$, forms a model of **U**. Inspection shows that the truth definition of the model is Δ_2 .

*6.2. The incompleteness theorems

Scott was the first to observe that one can give a model-theoretic proof of the First Incompleteness Theorem:

6.2.1. FIRST INCOMPLETENESS THEOREM. *There is a sentence φ such that (i) $\mathbf{PA} \not\vdash \varphi$ and (ii) $\mathbf{PA} \not\vdash \neg \varphi$.*

PROOF. Assume **PA** is complete. Then, since **PA** is true, $\mathbf{PA} \vdash \text{Con}_{\mathbf{PA}}$ and we can apply Theorem 6.1.1 to obtain a formula Tr_M which gives a truth definition for a model of **PA**. Choose φ by

$$\mathbf{PA} \vdash \varphi \leftrightarrow \neg \text{Tr}_M(' \varphi ').$$

We claim $\mathbf{PA} \not\vdash \varphi$, $\mathbf{PA} \not\vdash \neg \varphi$. For if $\mathbf{PA} \vdash \varphi$, then $\mathbf{PA} \vdash \text{Tr}_M(' \varphi ')$ so $\mathbf{PA} \vdash \neg \varphi$. Similarly, $\mathbf{PA} \vdash \neg \varphi$ implies $\mathbf{PA} \vdash \varphi$. $\square$

We shall discuss this proof a little later. First, we wish to prove the Second Incompleteness Theorem. For this, we need some notation:

6.2.2. DEFINITION. Let $\mathcal{M}, \mathcal{N}$ be models of **PA**. If $\mathcal{M}$ is definable in $\mathcal{N}$ (even in the weak sense that the atomic relations of $\mathcal{M}$ are $\mathcal{N}$ -definable), we write $\mathcal{M} <_d \mathcal{N}$.

The Hilbert–Bernays Completeness Theorem yields immediately the fact: If $\mathcal{N} \models \mathbf{PA} + \text{Con}_{\mathbf{PA}}$, then there is an $\mathcal{M}$ such that $\mathcal{M} <_d \mathcal{N}$.

The usefulness of this notion is given by the following.

6.2.3. LEMMA. *Let $\mathcal{M}, \mathcal{N}$ be models of **PA**, $\mathcal{M} <_d \mathcal{N}$. Then $\mathcal{M}$ is definably an end-extension of $\mathcal{N}$ — i.e. there is a unique $\mathcal{N}$ -definable isomorphic embedding of $\mathcal{N}$ into $\mathcal{M}$ as an initial segment of $\mathcal{M}$.*

PROOF. The proof is straightforward: $0_{\mathfrak{M}}$ obviously maps onto $0_{\mathfrak{M}}$. Extend the map, say F , by

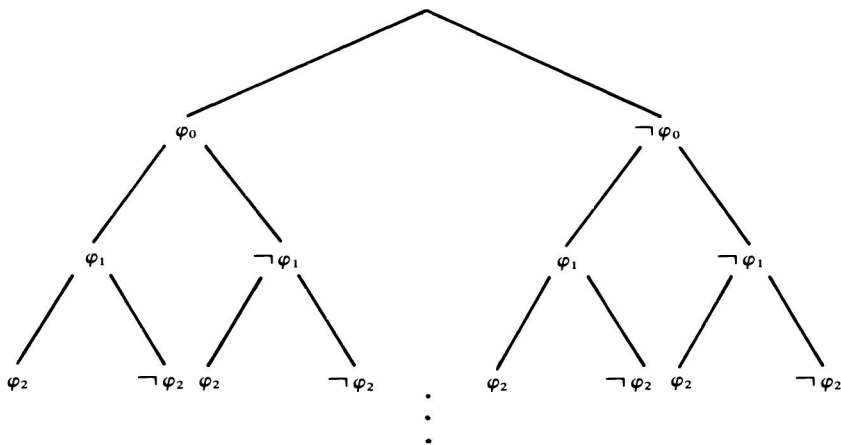
$$F(S_{\mathfrak{M}}x) = S_{\mathfrak{M}}(Fx),$$

where S denotes the successor functions of the models. The recursion equations in $\mathfrak{M}$ and induction in $\mathfrak{N}$ verify that F is an isomorphism of $\mathfrak{N}$ onto an initial segment of $\mathfrak{M}$. $\square$

Using this lemma, we may present Kreisel's proof of the following.

6.2.4. SECOND INCOMPLETENESS THEOREM. $\mathbf{PA} \not\vdash \text{Con}_{\mathbf{PA}}$.

PROOF. Let $\varphi_0, \varphi_1, \dots$ be an enumeration of sentences of the language described in the proof of 6.1.1. That proof can be viewed as an attempt to choose an infinite consistent path through the following tree:



We may assume for definiteness that the construction proceeds by taking the *leftmost* consistent path. Choose φ such that $\mathbf{PA} \vdash \varphi \leftrightarrow \neg \text{Tr}_{\mathfrak{M}}(\ulcorner \varphi \urcorner)$, for the truth definition, $\text{Tr}_{\mathfrak{M}}$, of the model constructed. Let $\varphi = \varphi_{n_0}$ in the enumeration. The tree, as defined to the n_0 -th level, is absolute. I.e. it is the same in every model. (Note: This is not true for the infinite tree simply because any non-standard model $\mathfrak{M}$ will encode a level for φ_N for non-standard integers N . But the *finite* trees are fixed.)

Assume $\mathbf{PA} \vdash \text{Con}_{\mathbf{PA}}$. Let $\mathfrak{N}_0 \models \mathbf{PA}$. Then there is a model, $\mathfrak{N}_1$, definable in $\mathfrak{N}_0$: $\mathfrak{N}_1 <_d \mathfrak{N}_0$. But $\mathfrak{N}_1$ is also a model of $\text{Con}_{\mathbf{PA}}$ and there is an $\mathfrak{N}_2 <_d \mathfrak{N}_1$. Repeating, we get an infinite sequence,

$$\mathfrak{N}_0 >_d \mathfrak{N}_1 >_d \mathfrak{N}_2 >_d \dots,$$

such that (say)

$$\mathfrak{N}_0 \models \varphi_{n_0}, \quad \mathfrak{N}_1 \models \neg \varphi_{n_0}, \quad \mathfrak{N}_2 \models \varphi_{n_0}, \dots$$

We now use construction to derive a contradiction. Given $\mathfrak{N}_i$, let $\varphi^i = \langle \varphi_{0^i}^e, \varphi_{1^i}^e, \dots, \varphi_{n_0^{i+1}}^e \rangle$ denote the portion of the path used in constructing $\mathfrak{N}_{i+1}$ — where $\varphi_j^0 = \varphi_j$, $\varphi_j^1 = \neg \varphi_j$, and $e_{ji} \in \{0, 1\}$. Recall that φ^i is the leftmost consistent path (as viewed) in $\mathfrak{N}_i$.

Either using facts that $\text{Pr}_{\text{PA}} \vdash \Sigma_1$ and that Σ_1 sentences are preserved under end-extensions, or using D2 and the fact that

$$\text{PA} + \text{Con}_{\text{PA}} \vdash \forall \psi (\text{Pr}_{\text{PA}}(\ulcorner \psi \urcorner) \rightarrow \text{Tr}_M(\ulcorner \psi \urcorner)),$$

one sees that φ^{i+1} can never lie to the left of φ^i . For, once $\mathfrak{N}_i$ says that a sequence is inconsistent, every resulting $\mathfrak{N}_j$ will also assert its inconsistency. Put differently, larger models can allow new proofs (even of inconsistencies) e.g. by means of non-standard axioms encoded by infinite integers; but they cannot erase old proofs.

Thus φ^{i+1} cannot lie to the left of φ^i . Furthermore, $\varphi^{i+1} \neq \varphi^i$ since

$$\varphi_{n_0^{i+1}}^{e_{n_0^{i+1}}} = \varphi_{n_0^{i+1}}^{1-e_{n_0^i}} \leftrightarrow \neg \varphi_{n_0^i}^{e_{n_0^i}}.$$

Thus the path φ^{i+1} lies properly to the right of φ^i .

But the tree determined by $\varphi_0, \dots, \varphi_{n_0}$ is finite and there are only 2^{n_0+1} different paths through this tree. This contradicts the assumption $\text{PA} \vdash \text{Con}_{\text{PA}}$ by which we obtained an infinite sequence of paths: $\varphi^0, \varphi^1, \dots$. $\square$

*6.3. Comments

With Theorems 6.2.1 and 6.2.4, we have gone full circle: We have gotten back to the results with which we began this chapter. The present proofs differ somewhat from the originals and it is worth making a few comparisons.

Let us first comment on the forms of the independent sentences given by the two proofs of the First Incompleteness Theorem. “The” sentence which asserts its own unprovability is

(i) unique up to provable equivalence;

(ii) Π_1 and hence true.

“The” sentence asserting its falsity in the model constructed is

(i') not unique — for, if $\varphi \leftrightarrow \neg \text{Tr}_M(\ulcorner \varphi \urcorner)$, then

$$\neg \varphi \leftrightarrow \neg \text{Tr}_M(\ulcorner \neg \varphi \urcorner);$$

(ii') Δ_2 and, by (i'), there is no obvious way of deciding its truth or falsity.

(ii') can be gotten around as follows: One of φ , $\neg\varphi$ is true. Let $\exists x \forall y \psi xy$ be the Σ_2 form of the true statement. Then, for some n , $\chi = \forall y \psi \bar{n}y$ is true. But $\mathbf{PA} \not\vdash \chi$ as one would then have $\mathbf{PA} \vdash \exists x \forall y \psi xy$. But $\mathbf{PA} \not\vdash \neg\chi$ since χ is true.

The model-theoretic proof of the First Incompleteness Theorem given here is similar to the classical one — for, once one assumes completeness, Tr_M is the same as $\text{Pr}_{\mathbf{PA}}$. The model-theoretic proof of the Second Incompleteness Theorem differs radically from the classical one and we note some differences in the sort of information they yield:

(i) The classical proof readily yields the formalized version, $\mathbf{PA} \vdash \text{Con}_{\mathbf{PA}} \rightarrow \text{Con}_{\mathbf{PA} + \neg \text{Con}_{\mathbf{PA}}}$. Further, it applies directly to weaker theories like $\mathbf{PRA}$.

(ii) While the classical proof yields the existence of *some* model in which $\text{Con}_{\mathbf{PA}}$ fails, the model-theoretic one shows that, for any presentation of the Henkin construction (as given by the encoding, the enumeration $\varphi_0, \varphi_1, \dots$, etc.), there is a number m such that, for *any* model $\mathfrak{N}$ of $\mathbf{PA}$, the sequence

$$(*) \quad \mathfrak{N} >_d \mathfrak{N}_1 >_d \dots,$$

determined by the given presentation, must stop after fewer than m steps with a model in which $\text{Con}_{\mathbf{PA}}$ is false. (Of course, by the classical proof, there is a presentation of the Henkin construction with a very short sequence $(*)$ — simply let $\varphi_0 = \neg \text{Con}_{\mathbf{PA}}$. The present proof works for all enumerations $\varphi_0, \dots$.)

References

The following is a very biased selection of the many papers on the topic of this chapter. It includes some papers whose contents were not discussed

FEFERMAN, S.

[1962] Transfinite recursive progressions of axiomatic theories, *J. Symbolic Logic*, **27**, 259–316.

GÖDEL, K.

[1931] Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I, *Monatsh. Math. Phys.*, **38**, 173–198.

HASENJÄGER, G.

[1953] Eine Bemerkung zu Henkin's Beweis für die Vollständigkeit des Prädikatenkalküls der ersten Stufe, *J. Symbolic Logic*, **18**, 42–48.

HILBERT, D. and P. BERNAYS

[1970] *Grundlagen der Mathematik*, I (Springer, Berlin, 2nd ed.).

JEROSLOW, R.G.

[1973] Redundancies in the Hilbert–Bernays derivability conditions for Gödel’s second incompleteness theorem, *J. Symbolic Logic*, **38**, 359–367.

KENT, C.F.

[1973] The relation of A to $\text{Prov}^1 A$ in the Lindenbaum sentence algebra, *J. Symbolic Logic*, **38**, 295–298.

KREISEL, G. and A. LEVY

[1968] Reflection principles and their use for establishing the complexity of axiomatic systems, *Z. Math. Logik Grundlagen Math.*, **14**, 97–142.

KREISEL, G. and G. TAKEUTI

[1974] Formally self-referential propositions in cut-free classical analysis and related systems, *Dissertationes Math.*, **118**, 1–50.

LÖB, M.H.

[1955] Solution of a problem of Leon Henkin, *J. Symbolic Logic*, **20**, 115–118.

MESCHKOWSKI, H.

[1973] *Hundert Jahre Mengenlehre* (Deutscher Taschenbuch Verlag; München).

REID, C.

[1970] *Hilbert* (Springer, Berlin).

ROSSER, J.B.

[1936] Extensions of some theorems of Gödel and Church, *J. Symbolic Logic*, **1**, 87–91.

SAMBIN, G.

[0000] An effective fixed-point theorem in intuitionistic diagonalizable algebras, *Studia Logica*, to appear.

SMORYNSKI, C.

[0000] ω -consistency and reflection, in: *Proceedings of the 1975 Logic Colloquium at Clermont-Ferrand*, to appear.

SOLOVAY, R.

[1976] Provability interpretations of modal logic, *Isr. J. Math.*, **25**, 287–304.

Proof Theory: Some Applications of Cut-Elimination

HELMUT SCHWICHTENBERG

Contents

1. Introduction	868
2. Cut-elimination for first-order logic	871
3. Transfinite induction .	876
4. Bounds from proofs of existential theorems .	884
5. Transfinite induction and the reflection principle	892
References	894

1. Introduction

1.1. Proof theory began with *Hilbert's Program*, which called for elementary consistency proofs for formalized mathematical theories **S**. Equivalently (under quite general conditions discussed in Chapter D.1) this program can be formulated as follows. Given a formalization in **S** of an abstract proof of an elementary assertion φ (example: proof of $n + m = m + n$, n, m variables for natural numbers, in an axiomatic set theory), can one always conclude from this by elementary means that φ is true? Or more precisely, can one give an elementary proof of the schema

$$(*) \quad \exists x \text{ Der}_S(x, \ulcorner \varphi \urcorner) \rightarrow \varphi,$$

where $\text{Der}_S(\cdot, \cdot)$ is a canonical representation of the derivation predicate for **S** and φ ranges over formulas corresponding to elementary assertions? By the well-known second incompleteness theorem of Gödel, discussed in Chapter D.1, $(*)$ is undervivable in **S**, provided **S** is sufficiently strong. Now since one would expect that a strong theory **S** contains at least formalizations of all "elementary" proofs, one may fairly say that this refutes Hilbert's Program in its original form. However, one can also try to extend the (originally quite vague) conception of an elementary proof and then look for such a proof of $(*)$ not formalizable in **S**; in fact, this was Hilbert's reaction to Gödel's result (cf. the introduction to HILBERT and BERNAYS [1934]). We shall not deal here with contributions to Hilbert's Program along these lines (for this, cf. e.g. SCHÜTTE [1960]), but rather concentrate on some less delicate questions which are derived from and closely related to Hilbert's Program.

1.1.1. A theory **S** is called *conservative* over a theory **T** if any formula of $L(\mathbf{T})$ (the language of **T**) derivable in **S** is already derivable in **T**. Note that this would be a corollary of the derivability of $(*)$ in **T** (under quite general conditions). There are numerous important and nontrivial examples of theories **S** conservative over a subtheory **T**. Some of these are discussed in Chapters D.4 and D.5. We shall give here a very simple example and show that first-order logic is conservative over its part which uses formulas of a restricted complexity only (cf. Section 2.8).

1.1.2. The schema $(*)$ (now taken with arbitrary φ) provides, generally, a proper extension of **S**. However, $(*)$ has a metamathematical character and its mathematical strength is difficult to judge. So one might ask for an *equivalent formulation of $(*)$ having a clear mathematical meaning*. This

question has been answered for a wide variety of theories S . We shall confine ourselves here to a basic example, namely (classical) arithmetic Z , and prove that in this case (a version of) $(*)$ is equivalent to the schema of transfinite induction up to ε_0 .

1.2. Our second starting point is a question which only more recently came to the attention of proof theorists (cf. KREISEL [1958]): “*What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?*” Again we shall confine ourselves to the discussion of a basic example, where the “restricted means” are those formalized in arithmetic Z . We shall obtain a complete answer to the above question, due to KREISEL [1952]. For some subsystems of analysis one can also get satisfactory answers to questions of the type above; for this we refer the reader to Chapter D.4.

1.3. From a more technical point of view, we survey some elementary applications of a basic technique in proof theory: the method of cut-elimination. This method is due to Gentzen and was later developed particularly by Schütte and Tait (cf. SCHÜTTE [1960] and TAIT [1968]). Other techniques frequently used in proof theory are adequately covered in other chapters in this volume. Especially important is the method of functional interpretation due to GÖDEL [1958], which is treated in Chapter D.5.

1.4. We now give a more detailed account of the content of the present chapter.

In Section 2 we prove the *Cut-Elimination Theorem* for first-order logic; as a corollary we obtain the conservative extension result mentioned above. The proof of this basic Cut-Elimination Theorem is set up in such a way that it can be easily generalized to many other cases where a cut-elimination argument is applied, in particular to those treated here.

In Section 3 we discuss for arithmetic Z the provability and unprovability of initial cases of transfinite induction. The result (due to GENTZEN [1943]) is well known: Given a natural well-ordering $<$ of order type ε_0 , then with respect to $<$ transfinite induction is provable up to any ordinal $< \varepsilon_0$, but not up to ε_0 itself.

The underderivability in Z of transfinite induction up to ε_0 will also follow from Gödel's second incompleteness theorem together with the fact that transfinite induction up to ε_0 suffices to prove the reflection principle for Z and hence the consistency of Z (cf. Section 5). Here we give a direct proof

of this underderivability result, using a cut-elimination argument. Technically, this provides an easy and convincing example of the usefulness of infinite derivations and the strength of the cut-elimination method when applied to infinite derivations.

In Section 4 we take up the question of Section 1.2. We first consider the special case of $\forall\exists$ -formulas. Suppose $\forall n \exists m \varphi(n, m)$ with $\varphi(n, m)$ quantifier-free is derivable in $\mathbf{Z}$. We shall show that then we can find a function F satisfying $\forall n \varphi(n, F(n))$ which has a somewhat limited rate of growth: F can be defined by primitive recursive operations and α -recursions for $\alpha < \varepsilon_0$.

We then turn to the general case of arbitrary $\mathbf{Z}$ -formulas. At first sight a generalization of the result for $\forall\exists$ -formulas seems to be impossible, since $\forall n \exists m \forall k (T(n, n, k) \rightarrow T(n, n, m))$ is derivable (in classical logic and hence) in $\mathbf{Z}$, but there is no recursive function F satisfying $\forall n \forall k (T(n, n, k) \rightarrow T(n, n, F(n)))$ (this would contradict the recursive undecidability of $\exists k T(n, n, k)$; T is Kleene's T -predicate). However, there is such a generalization, the so-called No-Counterexample-Interpretation due to KREISEL [1952]. To explain it let us first consider a formula of the above form, i.e. $\psi \equiv \forall n \exists m \forall k \varphi(n, m, k)$ with $\varphi(n, m, k)$ quantifier-free. Its negation is equivalent to $\exists n \forall m \exists k \neg \varphi(n, m, k)$ and hence (using the axiom of choice) also to $\exists n, f \forall m \neg \varphi(n, m, f(m))$; such n, f can be considered as providing a counterexample to the given formula ψ . So a way to express the content of ψ is to say that there is no such counterexample, i.e. that for any n, f we have $\exists m \varphi(n, m, f(m))$ (this formula is the Herbrand normal form of ψ), i.e. that there is a functional F such that $\forall n, f \varphi(n, F(n, f), f(F(n, f)))$ holds. Now the additional information we obtain from the fact that ψ is derivable in $\mathbf{Z}$ is that such a functional F can be found which again has a somewhat limited complexity: F can be defined by primitive recursive operations (in the sense of KLEENE [1959]) and α -recursions for some $\alpha < \varepsilon_0$, or — as we shall say — F is $< \varepsilon_0$ -recursive.

Generally, let ψ be an arbitrary $\mathbf{Z}$ -formula and let $\psi_H \equiv \exists m \psi^H(n, m, f)$ be its Herbrand normal form which is derivable in $\mathbf{Z}$ iff ψ is. (We use f for finite sequences of function variables and n, m for finite sequences of number variables.) The result then is that from the derivability of ψ in $\mathbf{Z}$ we can conclude that there are $< \varepsilon_0$ -recursive functionals F satisfying $\forall n, f \psi^H(n, F(n, f), f)$. We also prove that this result is the best possible in the sense that no smaller class of functionals suffices.

The proof involves a new point: it makes use of the fact that the cut-elimination procedure for infinite derivations is an effective operation.

More precisely, we show that for a natural coding of infinite derivations the cut-elimination procedure is given by a primitive recursive function.

In Section 5 we come back to the question asked in Section 1.1.2 and prove the result stated there (which is due to KREISEL and LÉVY [1968]). The proof is a formalization of the argument in Section 4, i.e. cut-elimination for codes of infinite derivations.

Acknowledgements: Parts of the present chapter are based on other sources, in particular TAIT [1968] (for the proof of the Cut-Elimination Theorem in Section 2) and SCHÜTTE [1960] (for the proof in Section 3 of the underivability of transfinite induction up to ε_0 in $\mathbf{Z}$). Also I want to thank S. Feferman, G. Kreisel, R. Statman and A.S. Troelstra for many helpful comments and suggestions; in particular, the idea to prove the No-Counterexample-Interpretation by means of a cut-elimination argument is due to Kreisel.

2. Cut-elimination for first-order logic

We prove this basic Cut-Elimination Theorem by a method due to Gentzen which is central for our later work: nearly all the results mentioned in the introduction will be obtained by generalizations of this method. Technically we shall follow TAIT [1968] quite closely, but with one exception: we shall avoid infinite formulas throughout (and later use infinite derivations only where they seem to be essential).

2.1. We use the ordinary *language* of first-order logic, for simplicity in the following version: formulas are built up from atomic and negated atomic formulas by means of $\wedge$, $\vee$, $\forall x$, $\exists x$. The negation $\neg\varphi$ of a formula φ is *defined* to be the formula obtained from φ by

- (i) putting a $\neg$ in front of any atomic formula,
- (ii) replacing $\wedge$, $\vee$, $\forall x$, $\exists x$ by $\vee$, $\wedge$, $\exists x$, $\forall x$, respectively, and
- (iii) dropping double negations.

This treatment of negation is possible since we assume classical logic throughout. Note that $\neg\neg\varphi$ is identical with φ , $\neg\neg\varphi \equiv \varphi$. As usual, we define $\varphi \rightarrow \psi$ to be $\neg\varphi \vee \psi$ and $\varphi \leftrightarrow \psi$ to be $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$. Let $|\varphi|$ (the *length* of φ) be defined as follows.

- (i) $|\varphi| = |\neg\varphi| = 0$, for φ atomic.
- (ii) $|\varphi \wedge \psi| = |\varphi \vee \psi| = \sup(|\varphi|, |\psi|) + 1$.
- (iii) $|\forall x \varphi(x)| = |\exists x \varphi(x)| = |\varphi(x)| + 1$.

Note that $|\neg\varphi| = |\varphi|$.

2.2. Logical rules

We shall derive finite sets of formulas, denoted by $\Gamma, \Delta, \Lambda, \Gamma(a), \dots$. The intended meaning of Γ is the disjunction of all formulas in Γ . We use the notation

$$\Gamma, \varphi \quad \text{for } \Gamma \cup \{\varphi\},$$

$$\Gamma, \Delta \quad \text{for } \Gamma \cup \Delta.$$

(i) *Normal rules*:

$$\mathbf{A} \quad \Gamma, \varphi, \neg \varphi \quad \text{if } \varphi \text{ is atomic.}$$

$$\mathbf{\wedge} \quad \frac{\Gamma, \varphi \quad \Gamma, \psi}{\Gamma, \varphi \wedge \psi}.$$

$$\mathbf{\vee}_0 \quad \frac{\Gamma, \varphi}{\Gamma, \varphi \vee \psi}, \quad \mathbf{\vee}_1 \quad \frac{\Gamma, \psi}{\Gamma, \varphi \vee \psi}.$$

$$\mathbf{\forall} \quad \frac{\Gamma, \varphi(x)}{\Gamma, \forall x \varphi(x)} \quad \text{if } x \text{ is not free in } \Gamma$$

(x is called eigenvariable of $\forall$).

$$\mathbf{\exists} \quad \frac{\Gamma, \varphi(s)}{\Gamma, \exists x \varphi(x)}.$$

(ii) *Cut-rule*:

$$\mathbf{Cut} \quad \frac{\Gamma, \varphi \quad \Gamma, \neg \varphi}{\Gamma}.$$

The *principal formulas* (p.f.) in $\mathbf{A}$ are φ and $\neg \varphi$. In $\mathbf{\wedge}$, $\mathbf{\vee}_i$, $\mathbf{\forall}$ and $\mathbf{\exists}$ the p.f. is $\varphi \wedge \psi$, $\varphi \vee \psi$, $\forall x \varphi(x)$ and $\exists x \varphi(x)$, respectively. $\mathbf{Cut}$ has no p.f. The *minor formula* (m.f.) in the premiss Γ, φ of $\mathbf{\wedge}$ is φ , and in the premiss Γ, ψ of $\mathbf{\wedge}$ it is ψ . In the premiss of $\mathbf{\vee}_0$, $\mathbf{\vee}_1$, $\mathbf{\forall}$ and $\mathbf{\exists}$ the m.f. is φ , ψ , $\varphi(x)$ and $\varphi(s)$, respectively. The m.f. in the premiss Γ, φ of $\mathbf{Cut}$ is φ , and in the premiss $\Gamma, \neg \varphi$ of $\mathbf{Cut}$ it is $\neg \varphi$. So any inference has the form

$$(*) \quad \frac{\Gamma, \varphi_i \quad \text{for all } i < k}{\Gamma, \Delta}$$

($0 \leq k \leq 2$), where Δ consists of the p.f. and φ_i is the m.f. in the i -th premiss. The formulas in Γ are called *side formulas* (s.f.) of (*).

Derivations are built up in tree form, as usual. More precisely, they are defined by the following induction. Consider an inference (*) as above and assume that derivations d_i of its premisses Γ, φ_i are given. Then $d = ((d_i)_{i < k}, (\varphi_i)_{i < k}, \Delta, \Gamma)$ is a derivation of the conclusion Γ, Δ of (*). The

inference considered is called the *last inference* of d . The d_i are called *direct subderivations* of d . We write $d \vdash \Gamma$ if d is a derivation of Γ , and $\vdash \Gamma$ if there is a derivation of Γ .

The *length* $|d|$ of a derivation d is inductively defined to be $\sup_{i < k} (|d_i| + 1)$ if the d_i , $i < k$, are the direct subderivations of d . Hence $|d| = 0$ if d has no direct subderivations. The *cut-rank* $\rho(d)$ of a derivation d is also defined by induction: Let d_i , $i < k$, be the direct subderivations of d . If the last inference of d is a cut with m.f. φ and $\neg\varphi$ let $\rho(d) := \sup(|\varphi| + 1, \sup_{i < k} \rho(d_i))$. Otherwise, let $\rho(d) := \sup_{i < k} \rho(d_i)$. Note that $\rho(d) = 0$ iff d is cut-free.

It is convenient to use the notions of free and bound occurrences of variables in derivations. A free occurrence of a variable x inside an occurrence of a formula in a derivation d is called *bound in d* if “below” that occurrence x is used as an eigenvariable of an inference $\forall$; otherwise this occurrence of x is called *free in d* . We use the notation $d, d(x), \dots$ for derivations where it is understood that there may be other free variables different from those actually shown.

2.3. Let d, Γ be obtained from a derivation d by adding Γ to the side formulas of all inferences in d . It is trivial to see that d, Γ is again a derivation provided no variable free in Γ is bound in d . The latter condition can always be assumed to hold if we identify derivations which differ only by a change of bound variables. Hence we have:

2.3.1. WEAKENING LEMMA. *If $d \vdash \Delta$, then $d, \Gamma \vdash \Gamma, \Delta$ with $|d, \Gamma| = |d|$ and $\rho(d, \Gamma) = \rho(d)$.*

2.4. Let $d(s)$ denote the result of substituting s for all free occurrences of x in $d(x)$ (note that some changes of bound variables in $d(x)$ may be necessary). Then we obviously have

2.4.1. SUBSTITUTION LEMMA. *If $d(x) \vdash \Gamma(x)$, then $d(s) \vdash \Gamma(s)$ with $|d(s)| = |d(x)|$ and $\rho(d(s)) = \rho(d(x))$.*

2.5. INVERSION LEMMA. (i) *If $d \vdash \Gamma$, $\varphi_0 \wedge \varphi_1$, then we can find $d_i \vdash \Gamma$, φ_i ($i = 0, 1$) with $|d_i| \leq |d|$ and $\rho(d_i) \leq \rho(d)$.*

(ii) *If $d \vdash \Gamma$, $\forall x \psi(x)$, then we can find $d_0 \vdash \Gamma$, $\psi(x)$ with $|d_0| \leq |d|$ and $\rho(d_0) \leq \rho(d)$.*

PROOF. The proofs of (i) and (ii) are almost identical, both by induction on

$|d|$. We restrict ourselves to (ii). Let φ be $\forall x \psi(x)$. We can assume $\varphi \notin \Gamma$, for otherwise the result follows by weakening, taking $d, \psi(x)$.

Case 1: φ is not a p.f. in the last inference of d . Then this inference has the form

$$\frac{\Lambda, \varphi, \psi_j \text{ for all } j < k}{\Lambda, \varphi, \Delta}$$

with m.f. ψ_j , p.f. Δ and s.f. Λ, φ , and $\Gamma = \Lambda, \Delta$. By the induction hypothesis $\vdash \Lambda, \psi(x), \psi_j$ for all $j < k$, with length $< |d|$ and cut-rank $\leq \rho(d)$. The result follows by the inference

$$\frac{\Lambda, \psi(x), \psi_j \text{ for all } j < k}{\Lambda, \psi(x), \Delta}$$

Case 2: φ is a p.f. in the last inference of d . We can assume that φ is a s.f. in the last inference of d , replacing d by d, φ if necessary. So that inference is of the form

$$\frac{\Gamma, \varphi, \psi(x)}{\Gamma, \varphi}$$

with m.f. $\psi(x)$, p.f. φ and s.f. Γ, φ . By the inductive hypothesis $\vdash \Gamma, \psi(x)$, with length $< |d|$ and cut-rank $\leq \rho(d)$. This completes the proof. $\square$

2.6. REDUCTION LEMMA. *Let $d_0 \vdash \Gamma, \varphi$ and $d_1 \vdash \Delta, \neg \varphi$, both with cut-rank $\rho(d_i) \leq |\varphi|$. Then we can find $d \vdash \Gamma, \Delta$ with $|d| \leq |d_0| + |d_1|$ and $\rho(d) \leq |\varphi|$.*

Of course we could derive Γ, Δ by an application of the cut-rule, but the resulting derivation would then have cut-rank $|\varphi| + 1$.

PROOF. The proof is by induction on $|d_0| + |d_1|$. Since $|\varphi| = |\neg \varphi|$ and $\neg \neg \varphi \equiv \varphi$, the lemma is symmetric with respect to the two given derivations.

Case 1: Either φ is not a p.f. in the last inference of d_0 or else $\neg \varphi$ is not a p.f. in the last inference of d_1 . By symmetry we can assume the former. Then the last inference of d_0 is of the form

$$\frac{\Lambda, \varphi, \psi_i \text{ for all } i < k}{\Lambda, \varphi, \Theta}$$

with m.f. ψ_i , p.f. Θ and s.f. Λ, φ , and $\Gamma = \Lambda, \Theta$. By the induction hypothesis $\vdash \Lambda, \Delta, \psi_i$ for all $i < k$ with length $< |d_0| + |d_1|$ and cut-rank $\leq |\varphi|$. The result then follows by the inference

$$\frac{\Lambda, \Delta, \psi_i \text{ for all } i < k}{\Lambda, \Delta, \Theta}$$

Case 2: φ is a p.f. in the last inference of d_0 , and $\neg \varphi$ is a p.f. in the last inference of d_1 .

Case 2.1.: φ or $\neg \varphi$ is atomic. Then the last (and only) inferences of d_0 and d_1 are instances of the rule A and hence Γ, Δ is also an instance of the rule A.

Case 2.2.: φ or $\neg \varphi$ is a disjunction $\varphi_0 \vee \varphi_1$. By symmetry we can assume the former, so $\neg \varphi$ is $\neg \varphi_0 \wedge \neg \varphi_1$. We can assume that φ is a s.f. of the last inference of d_0 , replacing d_0 by d_0, φ if necessary. So that inference is of the form

$$\frac{\Gamma, \varphi, \varphi_i}{\Gamma, \varphi}.$$

By the induction hypothesis $\vdash \Gamma, \Delta, \varphi_i$ with length $< |d_0| + |d_1|$ and cut-rank $\leq |\varphi|$. By the Inversion Lemma $\vdash \Delta, \neg \varphi_i$ with length $\leq |d_1| < |d_0| + |d_1|$ and cut-rank $\leq |\varphi|$. The result follows by an application of the cut rule.

Case 2.3.: φ or $\neg \varphi$ is of the form $\exists x \psi(x)$. Again we can assume the former (so $\neg \varphi$ is $\forall x \neg \psi(x)$), and also that φ is a s.f. of the last inference of d_0 . So that inference is of the form

$$\frac{\Gamma, \varphi, \psi(s)}{\Gamma, \varphi}.$$

By the induction hypothesis $\vdash \Gamma, \Delta, \psi(s)$ with length $< |d_0| + |d_1|$ and cut-rank $\leq |\varphi|$. By the Inversion Lemma $\vdash \Delta, \neg \psi(a)$ with length $\leq |d_1|$ and cut-rank $\leq |\varphi|$. By the Substitution Lemma $\vdash \Delta, \neg \psi(s)$ also with length $\leq |d_1|$ and cut-rank $\leq |\varphi|$. The result follows by an application of the cut rule. $\square$

2.7. CUT-ELIMINATION THEOREM. *If $d \vdash \Gamma$ and $\rho(d) > 0$, then we can find $d' \vdash \Gamma$ with $\rho(d') < \rho(d)$ and $|d'| \leq 2^{|d|}$.*

PROOF. The proof is by induction on $|d|$. We may assume that the last inference of d is a cut

$$\frac{\Gamma, \varphi \quad \Gamma, \neg \varphi}{\Gamma}$$

with $|\varphi| + 1 = \rho(d)$, for otherwise the result follows by the induction hypothesis (making use of the fact that our rules all have finitely many

premisses). So assume this. Let $d_0 \vdash \Gamma, \varphi$ and $d_1 \vdash \Gamma, \neg \varphi$ be the direct subderivations of d . By the induction hypothesis we have $d'_0 \vdash \Gamma, \varphi$ and $d'_1 \vdash \Gamma, \neg \varphi$, both with cut-rank $\rho(d'_i) \leq |\varphi|$ and length $|d'_i| \leq 2^{|d_i|}$. The result then follows by the Reduction Lemma, since $|d'_0| + |d'_1| \leq 2^{\sup(|d_0|, |d_1|)+1} = 2^{|d|}$. $\square$

Let $2_0^\xi = \xi$, $2_{k+1}^\xi = 2^{2_k^\xi}$.

2.7.1. COROLLARY. *If $d \vdash \Gamma$, then we can find a cut-free $d^* \vdash \Gamma$ with $|d^*| \leq 2_{\rho(d)}^{|d|}$.*

2.8. In this and the next subsection we prove two important consequences of the Cut-Elimination Theorem.

Define the relation “ ψ is a subformula of φ ” to be the smallest transitive and reflexive relation with the properties

- (i) φ_0, φ_1 are subformulas of $\varphi_0 \wedge \varphi_1, \varphi_0 \vee \varphi_1$, and
- (ii) $\varphi(s)$ is a subformula of $\forall x \varphi(x), \exists x \varphi(x)$.

The following is obvious.

2.8.1. SUBFORMULA PROPERTY. *Let d be a cut-free derivation of Γ . Then any formula occurring in d is a subformula of one of the formulas in Γ .*

Hence from the Cut-Elimination Theorem we can conclude that for any $d \vdash \Gamma$ we can find $d^* \vdash \Gamma$ containing only subformulas of formulas in Γ .

2.9. HERBRAND'S THEOREM. *Let $d \vdash \exists x \varphi(x)$ with $\varphi(x)$ quantifier-free. Then we can find terms $s_0, \dots, s_{n-1}$ and a derivation $d_0 \vdash \varphi(s_0), \dots, \varphi(s_{n-1})$.*

PROOF. We can assume that d is cut-free. Hence by the subformula property any instance of the rule $\exists$ in d has the p.f. $\exists x \varphi(x)$. Let $s_0, \dots, s_{n-1}$ be all the terms such that $\varphi(s_i)$ is the m.f. of such an instance of $\exists$. Now add $\varphi(s_0), \dots, \varphi(s_{n-1})$ to the side formulas of any inference in d , and cancel all occurrences of $\exists x \varphi(x)$ in d . It is easy to see that the resulting object is (essentially) the required derivation. $\square$

3. Transfinite induction

In this and the following sections we shall deal with (classical) arithmetic **Z**. We begin with a discussion of transfinite induction, particularly of the

question which initial cases of transfinite induction are derivable in $\mathbf{Z}$. By an extension of the cut-elimination argument in Section 2 we shall show that transfinite induction up to ε_0 is underivable in $\mathbf{Z}$. This provides a precise bound, since it is easy to see that for any $\alpha < \varepsilon_0$ transfinite induction up to α is provable in $\mathbf{Z}$ (cf. SCHÜTTE [1960] or Chapter D.4).

3.1. To fix notation we first describe our version of *arithmetic* $\mathbf{Z}$, which is in fact usual arithmetic plus free set and function variables. So we have number variables, set variables and for any $n > 0$ variables for n -place functions (countably many of each sort). They are denoted by k, m, n, p , by X, Y, Z , and by f, g, h , respectively. The *terms* of $\mathbf{Z}$ are built up from a constant 0 (for the number 0) and the number variables by means of the function symbols S (for successor), $+$, $\cdot$ and the function variables. The *atomic formulas* of $\mathbf{Z}$ are of the form $s = t$, $s < t$ or $s \in X$, where s, t are terms and X is a set variable. The *formulas* are built up from these as usual, using quantification on number variables only.

The *axioms* of $\mathbf{Z}$ are the usual axioms for 0, S , $<$ ($\neg n < 0$, $m < Sn \leftrightarrow (m < n \vee m = n)$), $+$, $\cdot$ and equality, and the induction schema

$$\varphi(0) \wedge \forall n (\varphi(n) \rightarrow \varphi(Sn)) \rightarrow \forall n \varphi(n),$$

where $\varphi(n)$ is an arbitrary formula of the language, possibly containing additional variables. The theorems of $\mathbf{Z}$ are those derivable from the axioms by classical logic.

The various sets and functions one wants to talk about in arithmetic can be introduced in *definitional* (and hence conservative) *extensions* of $\mathbf{Z}$. There is one type of these we are particularly interested in, the so-called recursive extensions of $\mathbf{Z}$. Such an extension occurs if

(i) we introduce a new set symbol M with the defining axiom $n \in M \leftrightarrow \varphi(n)$ where $\varphi(n)$ is quantifier-free, or

(ii) if we have derived $\exists m \varphi(n, m, f)$ with $\varphi(n, m, f)$ quantifier-free and then introduce a new functional symbol F with the defining axioms

$$\varphi(n, F(n, f), f), \quad m < F(n, f) \rightarrow \neg \varphi(n, m, f).$$

$\mathbf{Z}'$ is called a *recursive extension* of $\mathbf{Z}$ if it is obtained from $\mathbf{Z}$ by a finite sequence of definitional extensions of this sort. Recursive extensions of $\mathbf{Z}$ will also be denoted by $\mathbf{Z}$.

One can show that any primitive recursive function can be introduced in a recursive extension of $\mathbf{Z}$ (cf. SHOENFIELD [1967]). Conversely, any such function is certainly recursive. We will determine in Section 4 exactly which recursive functionals can be introduced in recursive extensions of $\mathbf{Z}$.

Obviously $\mathbf{Z}$ is a conservative extension of its part without function variables, or without set variables, or without both. These subsystems will also be denoted by $\mathbf{Z}$.

3.2. Natural well-orderings of order type ε_0

As is well known, the ordinals $< \varepsilon_0$ can be built up from 0 by means of the ordinal functions $\alpha + \beta$ and ω^α . This build-up is unique if one uses the Cantor normal form (cf. BACHMANN [1955]). Hence ordinals $< \varepsilon_0$ may be considered as finite objects and so they can be coded by natural numbers. It is easy to choose these codes in such a way that

(i) the coding provides a bijective mapping $\alpha \mapsto \ulcorner \alpha \urcorner$ from the ordinals $< \varepsilon_0$ onto the natural numbers,

(ii) the relation $n < m$ corresponding to the less-than relation between ordinals $< \varepsilon_0$ is primitive recursive, and

(iii) the number-theoretic functions corresponding to the ordinal functions $\alpha + \beta$, ω^α and their inverses are primitive recursive.

Obviously, any two codings with the properties (i)–(iii) will be primitive recursive isomorphic. Any of the corresponding $<$ -relations between natural numbers is called a *natural well-ordering of order type ε_0* . We choose one of them, denote it by $<$ and fix it for the following. We write $n \leq m$ for $n < m \vee n = m$.

3.3. Let $\text{Prog}(X)$ (“ X is progressive”) be the formula $\forall n (\forall m (m < n \rightarrow m \in X) \rightarrow n \in X)$. The axiom of transfinite induction up to ε_0 is

$$\text{TI}_{\varepsilon_0}(X) \quad \text{Prog}(X) \rightarrow \forall n (n \in X).$$

Here $m < n$ stands for $\langle m, n \rangle \in M$ where $\langle \cdot, \cdot \rangle$ is one of the usual primitive recursive pairing functions and M is a symbol for the primitive recursive set of pair-numbers $\langle m, n \rangle$ such that $m < n$ holds.

3.3.1. THEOREM (GENTZEN [1943]). $\text{TI}_{\varepsilon_0}(X)$ is underivable in arithmetic $\mathbf{Z}$.

The proof of this theorem will cover the rest of Section 3. In outline, it proceeds as follows. We first embed $\mathbf{Z}$ in a “semi-formal” system $\mathbf{Z}_\omega$, where induction is replaced by a rule with infinitely many premisses, the so-called ω -rule:

$$\frac{\Gamma, \Delta(\bar{i}_0, \dots, \bar{i}_{k-1}) \quad \text{for all } i_0, \dots, i_{k-1} < \omega}{\Gamma, \Delta(n_0, \dots, n_{k-1})}$$

where $\bar{i}$ is the i -th numeral, i.e. $S^i 0$. By a slight extension of the argument in Section 2 we will obtain a Cut-Elimination Theorem for $\mathbf{Z}_\infty$ which gives a bound on the length of the cut-free derivation in terms of length and cut-rank of the derivation we started with. In particular, if we started with (the image in $\mathbf{Z}_\infty$ of) a $\mathbf{Z}$ -derivation, then this length will be $< \varepsilon_0$. We will then extend $\mathbf{Z}$ by yet another infinitary rule, the so-called *progression rule* introduced by Schütte:

$$\text{Prog} \quad \frac{\Gamma, \bar{i} \in X \quad \text{for all } i < j}{\Gamma, s \in X}$$

where s is a closed term with numerical value j . It is easy to see that in $\mathbf{Z}_\infty + \text{Prog}$ one can give a derivation of $\text{Prog}(X)$, and that this derivation has a finite length. Again a Cut-Elimination Theorem with the same ordinal bounds holds for $\mathbf{Z}_\infty + \text{Prog}$. Now assume that $\text{TI}_{\varepsilon_0}(X)$ is derivable in $\mathbf{Z}$. Since $\text{Prog}(X)$ is derivable in $\mathbf{Z}_\infty + \text{Prog}$ with finite length, we can conclude that the formula $n \in X$ (with variable n) is cut-free derivable in $\mathbf{Z}_\infty + \text{Prog}$ with a length $\alpha < \varepsilon_0$. Hence also $\overline{\alpha + 1} \in X$ is derivable in $\mathbf{Z}_\infty + \text{Prog}$ with length α . But this is a contradiction, since from the form of the rules of $\mathbf{Z}_\infty + \text{Prog}$ it follows immediately that any cut-free derivation of $\overline{\beta} \in X$ has length β .

3.4. Cut-Elimination for $\mathbf{Z}_\infty$

3.4.1. Description of $\mathbf{Z}_\infty$

The *language* of $\mathbf{Z}_\infty$ is the same as for $\mathbf{Z}$; we can assume here that we do not have function variables. For notions connected with derivations we use the same notation as in Section 2.

A finite set Δ of formulas is called a $\mathbf{Z}_\infty$ -*axiom* if Δ consists of atomic or negated atomic formulas without number variables such that $\vee \Delta$ (the disjunction of the formulas in Δ) is a tautological consequence of substitution instances of the quantifier-free axioms of $\mathbf{Z}$.

The *normal rules* of $\mathbf{Z}_\infty$ are

$$\text{A} \quad \Gamma, \Delta \quad \text{if } \Delta \text{ is a } \mathbf{Z}_\infty\text{-axiom,}$$

the rules $\wedge$, $\vee_0$, $\vee_1$, $\forall$, $\exists$ listed in Section 2 and the ω -rule

$$\omega \quad \frac{\Gamma, \Delta(\bar{i}) \quad \text{for all } i}{\Gamma, \Delta(\mathbf{n})}$$

Furthermore, we have in $\mathbf{Z}_\infty$ the *cut-rule* Cut stated in Section 2.

Note that in the ω -rule we allow $\mathbf{n}$ to be empty. Also it is allowed that in $\Delta(\mathbf{n})$ no variable of $\mathbf{n}$ actually has a free occurrence. In these cases the

conclusion of the ω -rule is the same as its premiss(es). Such an instance of the ω -rule is called *improper*.

The *principal formulas* (p.f.) in Δ are all formulas in Δ . In the ω -rule the p.f. are all formulas in $\Delta(\mathbf{n})$. The *minor formulas* (m.f.) in the i -th premiss of the ω -rule are all formulas in $\Delta(\bar{i})$. So any inference now has the form

$$(*) \quad \frac{\Gamma, \Delta_i \text{ for all } i < \alpha}{\Gamma, \Delta}$$

($0 \leq \alpha \leq \omega$), where Δ consists of the p.f. and Δ_i consists of the m.f. in the i -th premiss. The formulas in Γ are again called *side formulas* (s.f.) of (*).

Derivations will now be infinite; they are defined as in Section 2.2. (In the case of the ω -rule we have to add information about the variables $\mathbf{n}$.) Also the other notions introduced in Section 2.2, particularly the *length* $|d|$ and the *cut-rank* $\rho(d)$ of a derivation d carry over with the same definitions. Note that $|d|$ is now a countable ordinal, and $\rho(d) \leq \omega$. We restrict ourselves throughout to derivations with only finitely many free and bound variables. The set of variables free in a derivation d is denoted by $\text{Var}(d)$.

3.4.2. EMBEDDING LEMMA. *For any φ derivable in $\mathbf{Z}$ we have a $\mathbf{Z}_\infty$ -derivation $d \vdash \varphi$ of length $|d| < \omega \cdot 2$ and cut-rank $\rho(d) < \omega$.*

This is easy to see for the axioms of $\mathbf{Z}$ (for induction one has to use the ω -rule), and it is trivially preserved by the logical rules.

3.4.3. We now extend the proof given in Section 2 of the Cut-Elimination Theorem for first-order logic to $\mathbf{Z}_\infty$. Obviously we have:

WEAKENING LEMMA. *If $d \vdash \Delta$, then $d, \Gamma \vdash \Gamma, \Delta$ with $|d, \Gamma| = |d|$, $\rho(d, \Gamma) = \rho(d)$ and $\text{Var}(d, \Gamma) = \text{Var}(d) \cup V$, where V is the set of variables free in Γ .*

Note that any closed term s has a numerical value i , and $s = \bar{i}$ is a $\mathbf{Z}_\infty$ -axiom.

EVALUATION LEMMA. *Let s, t be closed terms, both with the same value i . If $d \vdash \Gamma(s)$, then we can find $d_0 \vdash \Gamma(t)$ with $|d_0| = |d|$, $\rho(d_0) = \rho(d)$ and $\text{Var}(d_0) = \text{Var}(d)$.*

It is easily seen that this holds for instances of the rule A and is preserved by the other rules.

SUBSTITUTION LEMMA. *If $d(n) \vdash \Gamma(n)$, then $d(s) \vdash \Gamma(s)$ with $|d(s)| \leq |d(n)|$, $\rho(d(s)) \leq \rho(d(n))$ and $\text{Var}(d(s)) \subseteq (\text{Var}(d) - \{n\}) \cup V$, where V is the set of variables free in s .*

The proof is by induction on $|d(n)|$. The only case which requires some argument is that in which the last inference of $d(n)$ is an instance of the ω -rule of the form

$$\frac{\Gamma(n, \mathbf{m}, \mathbf{p}), \Delta(\bar{i}, \bar{j}, \mathbf{p}) \text{ for all } i, j}{\Gamma(n, \mathbf{m}, \mathbf{p}), \Delta(n, \mathbf{m}, \mathbf{p})}$$

where $\mathbf{m}, \mathbf{p}$ include all variables free in $s = s(\mathbf{m}, \mathbf{p})$ (but $\Gamma(n, \mathbf{m}, \mathbf{p})$, $\Delta(n, \mathbf{m}, \mathbf{p})$ may contain free variables other than those shown). By the induction hypothesis,

$$\vdash \Gamma(\bar{i}, \mathbf{m}, \bar{\mathbf{k}}), \Delta(\bar{i}, \bar{j}, \bar{\mathbf{k}}) \text{ for all } i, j, \mathbf{k}$$

with length $< |d(n)|$ and cut-rank $\leq \rho(d(n))$. From some of these derivations we obtain by the Evaluation Lemma,

$$\vdash \Gamma(s(\bar{j}, \bar{\mathbf{k}}), \mathbf{m}, \bar{\mathbf{k}}), \Delta(s(\bar{j}, \bar{\mathbf{k}}), \bar{j}, \bar{\mathbf{k}}) \text{ for all } j, \mathbf{k}$$

without raising length or cut-rank. The result follows by an application of the ω -rule.

INVERSION LEMMA. (i) *If $d \vdash \Gamma$, $\varphi_0 \wedge \varphi_1$, then we can find $d_i \vdash \Gamma$, φ_i ($i = 0, 1$) with $|d_i| \leq |d|$, $\rho(d_i) \leq \rho(d)$ and $\text{Var}(d_i) \subseteq \text{Var}(d)$.*

(ii) *If $d \vdash \Gamma$, $\forall n \psi(n)$, then we can find $d_0 \vdash \Gamma$, $\psi(n)$ with $|d_0| \leq |d|$, $\rho(d_0) \leq \rho(d)$ and $\text{Var}(d_0) \subseteq \text{Var}(d) \cup \{n\}$.*

The proofs of (i) and (ii) are almost identical, both by induction on $|d|$. We restrict ourselves to (ii). The only subcase not similar to 2.5 is where the last inference of d is an instance of the ω -rule. Then that inference is of the form

$$\frac{\Lambda(\mathbf{m}), \varphi(\mathbf{m}), \Delta(\bar{i}), \varphi(\bar{i}) \text{ for all } i}{\Lambda(\mathbf{m}), \Delta(\mathbf{m}), \varphi(\mathbf{m})}$$

with m.f. $\Delta(\bar{i})$, $\varphi(\bar{i})$, p.f. $\Delta(\mathbf{m})$, $\varphi(\mathbf{m})$ and s.f. $\Lambda(\mathbf{m})$, $\varphi(\mathbf{m})$, and $\Gamma \equiv \Lambda(\mathbf{m})$, $\Delta(\mathbf{m})$, $\varphi \equiv \varphi(\mathbf{m})$. By two applications of the induction hypothesis

$$\vdash \Lambda(\mathbf{m}), \psi(n, \mathbf{m}), \Delta(\bar{i}), \psi(n, \bar{i}) \text{ for all } i$$

with length $< |d|$ and cut-rank $\leq \rho(d)$. The result follows by an application of the ω -rule.

REDUCTION LEMMA. *Let $d_0 \vdash \Gamma$, φ and $d_1 \vdash \Delta$, $\neg \varphi$, both with cut-rank $\rho(d_i) \leq |\varphi|$. Then we can find $d \vdash \Delta$, Γ with $\rho(d) \leq |\varphi|$, $|d| \leq |d_0| \# |d_1|$ and $\text{Var}(d) \subseteq \text{Var}(d_0) \cup \text{Var}(d_1)$.*

Here $\#$ denotes the natural (or Hessenberg) sum of ordinals (cf. BACHMANN [1955]); $\#$ is strictly monotonic in both arguments.

The proof is by induction on $|d_0| \# |d_1|$. Again the only (sub-) case not similar to 2.6 is where φ is a p.f. in the last inference of d_0 , and $\neg \varphi$ is a p.f. in the last inference of d_1 , and the last inference of d_0 or d_1 is an instance of the ω -rule. By symmetry we can assume the former. We can also assume that φ is a s.f. of the last inference of d_0 , replacing d_0 by d_0, φ if necessary. So that inference is of the form

$$\frac{\Lambda(m), \varphi(m), \Theta(\bar{i}), \varphi(\bar{i}) \text{ for all } i}{\Lambda(m), \Theta(m), \varphi(m)}$$

with m.f. $\Theta(\bar{i}), \varphi(\bar{i})$, p.f. $\Theta(m), \varphi(m)$ and s.f. $\Lambda(m), \varphi(m)$, and $\Gamma \equiv \Lambda(m), \Theta(m), \varphi \equiv \varphi(m)$. By the Substitution Lemma $\vdash \Gamma(\bar{i}), \varphi(\bar{i})$ for all i , with length $< |d_0|$ and cut-rank $\leq |\varphi|$, and also $\vdash \Delta(\bar{i}), \neg \varphi(\bar{i})$ for all i , with length $\leq |d_1|$ and cut-rank $\leq |\varphi|$. By the induction hypothesis $\vdash \Gamma(\bar{i}), \Delta(\bar{i})$ for all i with length $< |d_0| \# |d_1|$ and cut-rank $\leq |\varphi|$. The result follows by an application of the ω -rule. This completes the proof of the Reduction Lemma. $\square$

Let $\varepsilon(\alpha)$ be the α -th ε -number.

CUT-ELIMINATION THEOREM. (i) *If $d \vdash \Gamma$ with $\rho(d) = \zeta + 1$, then we can find $d' \vdash \Gamma$ with $\rho(d') \leq \zeta$, $|d'| \leq 2^{|d|}$ and $\text{Var}(d') \subseteq \text{Var}(d)$.*

(ii) *If $d \vdash \Gamma$ with $\rho(d) = \omega$, then we can find $d' \vdash \Gamma$ with $\rho(d') = 0$, $|d'| \leq \varepsilon(|d|)$ and $\text{Var}(d') \subseteq \text{Var}(d)$.*

PROOF. (i) As in 2.7.

(ii) By induction on $|d|$. We may assume that the last inference of d is a cut

$$\frac{\Gamma, \varphi \quad \Gamma, \neg \varphi}{\Gamma}$$

for otherwise the result follows by the induction hypothesis. So assume this. By the induction hypothesis we have $d_0 \vdash \Gamma, \varphi$ and $d_1 \vdash \Gamma, \neg \varphi$, both cut-free and with length $|d_i| < \varepsilon(|d|)$. The result then follows by applying (i) $|\varphi|$ times. $\square$

COROLLARY. *If $d \vdash \Gamma$, then we can find a cut-free $d^* \vdash \Gamma$ with $|d^*| \leq 2_{\rho(d)}^{|d|}$ if $\rho(d) < \omega$, and $|d^*| \leq \varepsilon(|d|)$ if $\rho(d) = \omega$.*

3.5. Cut-Elimination for $\mathbf{Z}_\infty + \text{Prog}$

We add to $\mathbf{Z}_\infty$ the following *progression rule*:

$$\text{Prog} \quad \frac{\Gamma, \bar{t} \in X \quad \text{for all } i < j}{\Gamma, s \in X} \quad \begin{array}{l} \text{for } s \text{ a closed term} \\ \text{with value } j. \end{array}$$

The p.f. in Prog is $s \in X$, and the m.f. in the i -th premiss is $\bar{t} \in X$. Now all the definitions, lemmas and proofs of Section 3.4 carry over almost word for word. Only part of the proof of the Reduction Lemma must be extended slightly: So let φ be a p.f. in the last inference of d_0 , $\neg \varphi$ be a p.f. in the last inference of d_1 and φ be atomic. Let further the last inference in d_0 be Prog and in d_1 be A. We can assume that φ is a s.f. in the last inference of d_0 ; hence it has the form

$$\frac{\Gamma, s \in X, \bar{t} \in X \quad \text{for all } i < j}{\Gamma, s \in X} \quad \begin{array}{l} s \text{ a closed term} \\ \text{with value } j. \end{array}$$

The last (and only) inference of d_1 is an instance $\Delta, \neg(s \in X)$ of the rule A. Now it is easy to see that then either

- (i) $t \in X$ is in Δ for some closed t with value j , or
- (ii) Δ is already an instance of the rule A.

In the latter case the result follows by weakening. In the former case we have by the induction hypothesis $\vdash \Gamma, \Delta, t \in X, \bar{t} \in X$ for all $i < j$, with length $< |d_0|$ and cut-rank 0. The result follows by an application of the rule Prog.

3.6. Underivability of $\text{TI}_{\varepsilon_0}(X)$ in $\mathbf{Z}$

3.6.1. LEMMA. *In $\mathbf{Z}_\infty + \text{Prog}$ we can derive $\text{Prog}(X)$ with finite length and cut-rank.*

We give an informal argument which can be easily transformed into a derivation in $\mathbf{Z}_\infty + \text{Prog}$.

Recall $\text{Prog}(X) \equiv \forall n (\forall m (m < n \rightarrow m \in X) \rightarrow n \in X)$. For any $i < j$ we have $\forall m (m < \bar{j} \rightarrow m \in X) \rightarrow \bar{t} \in X$. Hence by the progression rule $\forall m (m < \bar{j} \rightarrow m \in X) \rightarrow \bar{j} \in X$. Hence $\text{Prog}(X)$ by the ω -rule.

3.6.2. LEMMA. *Let d be a cut-free derivation in $\mathbf{Z}_\infty + \text{Prog}$ of $\overline{\beta_1} \in X, \dots, \overline{\beta_k} \in X$. Then d has length $\geq \min(\beta_1, \dots, \beta_k)$.*

This follows immediately from the form of the rules of $\mathbf{Z}_\infty + \text{Prog}$; use induction on $|d|$. The whole derivation must consist of instances of the rule Prog and of improper instances of the ω -rule.

3.6.3. Now assume $\text{TI}_{\varepsilon_0}(X)$ is derivable in $\mathbf{Z}$. Recall that $\text{TI}_{\varepsilon_0}(X) \equiv \text{Prog}(X) \rightarrow \forall n (n \in X)$. By 3.4.2 and 3.6.1 we then have a $\mathbf{Z}_\infty + \text{Prog}$ -derivation of $n \in X$ (with variable n) with length $< \omega \cdot 2$ and finite cut-rank. By the Cut-Elimination Theorem for $\mathbf{Z}_\infty + \text{Prog}$ we obtain a cut-free derivation of $n \in X$ in $\mathbf{Z}_\infty + \text{Prog}$ with length $\alpha < \varepsilon_0$. Hence by the Substitution Lemma we should also have a cut-free derivation of $\lceil \alpha + 1 \rceil \in X$ in $\mathbf{Z}_\infty + \text{Prog}$ with length α . This contradicts 3.6.2.

4. Bounds from proofs of existential theorems

We now take up the question “What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?” As before, we restrict ourselves to arithmetic $\mathbf{Z}$, where one can get a satisfactory answer; cf. Section 1.4 for a summary of the results. Using the terminology of Section 3.1 we can also summarize the results as follows. We show that a functional F of level ≤ 2 (i.e. with number and function arguments) can be introduced in a recursive extension of $\mathbf{Z}$ iff F is $< \varepsilon_0$ -recursive, i.e. F can be defined by the (Kleene) primitive recursive operations and α -recursions for $\alpha < \varepsilon_0$.

4.1. $< \varepsilon_0$ -recursive functionals

A functional F of level ≤ 2 is called *primitive recursive in Kleene's sense* iff it can be defined by means of schemata (i)–(v) below. Here $\mathbf{n} = n_0, \dots, n_{p-1}$ is a sequence of number variables and $\mathbf{f} = f_0, \dots, f_{q-1}$ is a sequence of function variables.

- (i) (Identity) $F(\mathbf{n}, \mathbf{f}) = n_i$ (for $i < p$).
- (ii) (Function application) $F(\mathbf{n}, \mathbf{f}) = f_i(n_{j_0}, \dots, n_{j_{k-1}})$ (for $i < q$ and $j_0, \dots, j_{k-1} < p$).
- (iii) (Successor) $F(\mathbf{n}, \mathbf{f}) = n_i + 1$ (for $i < p$).
- (iv) (Substitution) $F(\mathbf{n}, \mathbf{f}) = G(H_0(\mathbf{n}, \mathbf{f}), \dots, H_{k-1}(\mathbf{n}, \mathbf{f}), K_0(\cdot, \mathbf{n}, \mathbf{f}), \dots, K_{l-1}(\cdot, \mathbf{n}, \mathbf{f}))$.
- (v) (Primitive recursion) $F(0, \mathbf{m}, \mathbf{f}) = G(\mathbf{m}, \mathbf{f}), \quad F(n+1, \mathbf{m}, \mathbf{f}) = H(F(n, \mathbf{m}, \mathbf{f}), n, \mathbf{m}, \mathbf{f})$.

In (iv), $K_j(\cdot, \mathbf{n}, \mathbf{f})$ means $\lambda x K_j(x, \mathbf{n}, \mathbf{f})$. Note that $F(\mathbf{n}, \mathbf{f})$ is always a natural number.

Let α be an ordinal $< \varepsilon_0$ and let $<$ be our natural well-ordering of order type ε_0 (cf. Section 3.2). By α -recursion we mean the following definition schema.

(vi) (α -Recursion) For $n < \lceil \alpha \rceil$,

$$F(n, m, f) = G(n, m, (F \upharpoonright n)(\cdot, m, f), f)$$

where

$$(F \upharpoonright n)(i, m, f) := \begin{cases} F(i, m, f) & \text{if } i < n, \\ 0 & \text{otherwise.} \end{cases}$$

For $\lceil \alpha \rceil \leq n$, $F(n, m, f) := 0$.

A functional F of level ≤ 2 is called $< \varepsilon_0$ -recursive iff F can be defined by the primitive recursive operations (i)–(v) and α -recursions for $\alpha < \varepsilon_0$. The class of $< \varepsilon_0$ -recursive functionals of level ≤ 2 is denoted by $\text{Rec}_{< \varepsilon_0}$.

4.2. THEOREM (KREISEL [1952]). *If $\forall n \exists m \varphi(n, m)$ is derivable in $\mathbf{Z}$ with $\varphi(n, m)$ quantifier-free and without free variables other than those shown, then we can find a function $F \in \text{Rec}_{< \varepsilon_0}$ such that $\forall n \varphi(n, F(n))$ holds.*

4.2.1. We first sketch the proof. So let a $\mathbf{Z}$ -derivation of $\forall n \exists m \varphi(n, m)$ or equivalently of $\exists m \varphi(n, m)$ be given. As in 3.4.2 we can transform this $\mathbf{Z}$ -derivation into an infinite $\mathbf{Z}_\infty$ -derivation $d(n) \vdash \exists m \varphi(n, m)$ with length $|d(n)| < \omega \cdot 2$ and finite cut-rank. Furthermore, as in 3.4.3, we can transform $d(n)$ into a cut-free $\mathbf{Z}_\infty$ -derivation $d^*(n) \vdash \exists m \varphi(n, m)$ with length $|d^*(n)| < \varepsilon_0$. By the Substitution Lemma in 3.4.3 we obtain for any i a $\mathbf{Z}_\infty$ -derivation $d^*(\bar{i}) \vdash \exists m \varphi(\bar{i}, m)$ also with length $|d^*(\bar{i})| < \varepsilon_0$. Now from the form of the normal rules of $\mathbf{Z}_\infty$ it is clear that $d^*(\bar{i})$ contains only subformulas (cf. 2.8) of $\exists m \varphi(\bar{i}, m)$. We may assume that $d^*(\bar{i})$ contains no free variable (otherwise substitute 0 for any variable free in $d^*(\bar{i})$). Hence all instances of the ω -rule in $d^*(\bar{i})$ must be improper (cf. 3.4.1) and so we may as well cancel them. This yields a cut-free $d^{**} \vdash \exists m \varphi(\bar{i}, m)$ which does not involve the ω -rule. To d^{**} we can apply the same argument as in the proof of Herbrand's Theorem 2.9 and obtain closed terms $s_0, \dots, s_{k-1}$ and a derivation of $\varphi(\bar{i}, s_0), \dots, \varphi(\bar{i}, s_{k-1})$. At least one of these formulas must be true. The value at the argument i of the function F we have to construct is to be the (say) least numerical value of some s_j such that $\varphi(\bar{i}, s_j)$ is true.

What still remains to be shown is that this F is $< \varepsilon_0$ -recursive. For this we use an “effective” counterpart of the above construction, where we work with codes for $\mathbf{Z}_\infty$ -derivations instead of using the $\mathbf{Z}_\infty$ -derivations themselves.

4.2.2. Codes for $\mathbf{Z}_\infty$ -derivations

The codes will be natural numbers. They are defined inductively, corresponding to the inductive build-up of $\mathbf{Z}_\infty$ -derivations. The inductive definition is trivial for the finite rules $\mathbf{A}$, $\wedge$, $\vee_0$, $\vee_1$, $\forall$, $\exists$, Cut . However, for the ω -rule there is a difficulty since then we in general have infinitely many premisses. The idea now is to assume that the codes for the premisses can be enumerated by a primitive recursive function, and to use a code (or primitive recursive index) of such an enumeration function to construct a code of the whole derivation. Another essential point is that our codes should contain sufficient information about the coded derivation. In particular, if a number u codes a derivation d , then we want to be able to read off primitive recursively from u

- (i) the name of the last inference of d and its p.f., m.f. and s.f. (and hence its conclusion),
- (ii) a bound for the length $|d|$,
- (iii) a bound for the cut-rank $\rho(d)$, and
- (iv) a bound for the (finite) set of variables free in d .

The corresponding primitive recursive functions will be denoted by $\text{Rule}(u)$, $\text{p.f.}(u)$, $\text{m.f.}(u)$, $\text{s.f.}(u)$, $\text{End}(u)$, $|u|$, $\text{Rank}(u)$ and $\text{Var}(u)$, respectively.

We do not write out all cases of the inductive definition of the predicate $u \in \text{Code}$ (u is a code for a $\mathbf{Z}_\infty$ -derivation), but rather give two examples corresponding to the rule Cut and the ω -rule.

Cut : If $u, v \in \text{Code}$, $\text{End}(u) = \langle \Gamma, \varphi \rangle$, $\text{End}(v) = \langle \Gamma, \neg \varphi \rangle$ and $|u|, |v| < a$, then $\langle \langle \text{Cut} \rangle, \langle \varphi \rangle, \langle \Gamma \rangle, a, u, v \rangle \in \text{Code}$.

ω -rule: If, for any i , $[e](i) =: u_i \in \text{Code}$, $\text{End}(u_i) = \langle \Gamma, \Delta(\bar{i}) \rangle$, $|u_i| < a$, $\text{Rank}(u_i) \leq k$ and $\text{Var}(u_i) \subseteq^* b$, then $\langle \langle \omega \rangle, \langle \Delta(\bar{n}) \rangle, \langle \bar{n} \rangle, \langle \Gamma \rangle, a, k, b, e \rangle \in \text{Code}$.

Here $[e]$ denotes the primitive recursive function coded by e . $[\dots]$ denotes as usual a natural code for the finite object $\dots$; $\subseteq^*$ corresponds (under the relevant coding of finite sets of variables) to $\subseteq$; $\langle x_0, \dots, x_{l-1} \rangle$ is a primitive recursive coding of finite sequences of natural numbers with primitive recursive inverses $(x)_i$, i.e. $\langle (x_0, \dots, x_{l-1}) \rangle_i = x_i$ for $i < l$. We also skip the (trivial) primitive recursive definitions of the functions $\text{Rule}(u), \dots$ mentioned above.

4.2.3. It is easy to see that all $\mathbf{Z}_\infty$ -derivations obtained by embedding $\mathbf{Z}$ in $\mathbf{Z}_\infty$ (cf. 3.4.2) can be coded, and that any such code has length $|u| < |\omega \cdot 2|$.

4.2.4. We now show that to the operations on $\mathbf{Z}_\infty$ -derivations defined in

3.4.3 (weakening, substitution, etc.) there correspond primitive recursive functions on the codes. This will follow by easy applications of the Primitive Recursion Theorem of KLEENE [1958]. The lemmas are stated in the order they can be proved. We shall only sketch the proof for one of them (a typical example).

WEAKENING LEMMA. *We have a primitive recursive function Weak such that for any $u \in \text{Code}$ and any Γ the following holds.*

- (i) $\text{Weak}(u, \ulcorner \Gamma \urcorner) =: u_0 \in \text{Code}$,
- (ii) $\text{End}(u_0) = \ulcorner \Gamma, \Delta \urcorner$ if $\text{End}(u) = \ulcorner \Delta \urcorner$,
- (iii) $|u_0| = |u|$,
- (iv) $\text{Rank}(u_0) = \text{Rank}(u)$, and
- (v) $\text{Var}(u_0) = \text{Var}(u) \cup^* V^*$ with V the set of variables free in Γ .

EVALUATION LEMMA. *We have a primitive recursive function Eval such that for any $u \in \text{Code}$, $\Gamma(n)$, variable n and closed terms s, t with the same value the following holds.*

- (i) $\text{Eval}(u, \ulcorner \Gamma(n) \urcorner, \ulcorner n \urcorner, \ulcorner s \urcorner, \ulcorner t \urcorner) =: u_0 \in \text{Code}$,
- (ii) $\text{End}(u_0) = \ulcorner \Gamma(t) \urcorner$ if $\text{End}(u) = \ulcorner \Gamma(s) \urcorner$,
- (iii) $|u_0| = |u|$,
- (iv) $\text{Rank}(u_0) = \text{Rank}(u)$, and
- (v) $\text{Var}(u_0) = \text{Var}(u)$.

SUBSTITUTION LEMMA. *We have a primitive recursive function Sub such that for any $u \in \text{Code}$, variable n and term s the following holds.*

- (i) $\text{Sub}(u, \ulcorner n \urcorner, \ulcorner s \urcorner) =: u_0 \in \text{Code}$,
- (ii) $\text{End}(u_0) = \ulcorner \Gamma(s) \urcorner$ if $\text{End}(u) = \ulcorner \Gamma(n) \urcorner$,
- (iii) $|u_0| \leq |u|$,
- (iv) $\text{Rank}(u_0) \leq \text{Rank}(u)$, and
- (v) $\text{Var}(u_0) \subseteq^* (\text{Var}(u) - \{n\}^*) \cup^* V^*$ where V is the set of variables free in s .

For the proof one has to construct a primitive recursive function (also by the Primitive Recursion Theorem) corresponding to the change of bound variables in $\mathbf{Z}_\infty$ -derivations.

INVERSION LEMMA. (1) *We have primitive recursive functions Inv_i ($i = 0, 1$) such that for any $u \in \text{Code}$ and conjunction $\varphi_0 \wedge \varphi_1$ the following holds.*

- (i) $\text{Inv}_i(u, \ulcorner \varphi_0 \wedge \varphi_1 \urcorner) =: u_i \in \text{Code}$,
- (ii) $\text{End}(u_i) = \ulcorner \Gamma, \varphi_i \urcorner$ if $\text{End}(u) = \ulcorner \Gamma, \varphi_0 \wedge \varphi_1 \urcorner$ with $\varphi_0 \wedge \varphi_1$ not in Γ ,
- (iii) $|u_i| \leq |u|$,

(iv) $\text{Rank}(u_i) \leq \text{Rank}(u)$, and

(v) $\text{Var}(u_i) \subseteq^* \text{Var}(u)$.

(2) We have a primitive recursive function Inv such that for any $u \in \text{Code}$ and generalization $\forall n \psi(n)$ the following holds.

(i) $\text{Inv}(u, \ulcorner \forall n \psi(n) \urcorner) =: u_0 \in \text{Code}$,

(ii) $\text{End}(u_0) = \ulcorner \Gamma, \psi(n) \urcorner$ if $\text{End}(u) = \ulcorner \Gamma, \forall n \psi(n) \urcorner$ with $\forall n \psi(n)$ not in Γ ,

(iii) $|u_0| \leq |u|$,

(iv) $\text{Rank}(u_0) \leq \text{Rank}(u)$, and

(v) $\text{Var}(u_0) \subseteq^* \text{Var}(u) \cup^* \{n\}^*$.

REDUCTION LEMMA. We have a primitive recursive function Red such that for any $u_0, u_1 \in \text{Code}$ and formula φ with $\text{Rank}(u_i) \leq |\varphi|$ ($i = 0, 1$) the following holds.

(i) $\text{Red}(u_0, u_1, \ulcorner \varphi \urcorner) =: u \in \text{Code}$,

(ii) $\text{End}(u) = \ulcorner \Gamma, \Delta \urcorner$ if $\text{End}(u_0) = \ulcorner \Gamma, \varphi \urcorner$ with φ not in Γ and $\text{End}(u_1) = \ulcorner \Delta, \neg \varphi \urcorner$ with $\neg \varphi$ not in Δ ,

(iii) $\text{Rank}(u) \leq |\varphi|$,

(iv) $|u| \leq \ulcorner \xi_0 \neq \xi_1 \urcorner$ if $|u_i| = \ulcorner \xi_i \urcorner$, and

(v) $\text{Var}(u) \subseteq^* \text{Var}(u_0) \cup^* \text{Var}(u_1)$.

CUT-ELIMINATION THEOREM. We have a primitive recursive function Elim such that for any $u \in \text{Code}$ with $\text{Rank}(u) = k + 1$ the following holds.

(i) $\text{Elim}(u) =: u' \in \text{Code}$,

(ii) $\text{End}(u') = \text{End}(u)$,

(iii) $|u'| \leq 2^{|\xi|}$ with $\ulcorner \xi \urcorner := |u|$,

(iv) $\text{Rank}(u') \leq k$, and

(v) $\text{Var}(u') \subseteq^* \text{Var}(u)$.

PROOF. By the Primitive Recursion Theorem we can define a primitive recursive function Elim with code e as follows.

Case 1. $\text{Rule}(u) = \ulcorner \text{Cut} \urcorner$. Let $\text{m.f.}(u) = \{\varphi, \neg \varphi\}^*$.

Subcase 1.1. $|\varphi| + 1 < \text{Rank}(u)$. Define $\text{Elim}(u) = \langle (u)_0, (u)_1, (u)_2, \ulcorner 2^{\xi_1} \urcorner, \text{Elim}((u)_4), \text{Elim}((u)_5) \rangle$ where $\ulcorner \xi^1 \urcorner = (u)_3$.

Subcase 1.2. $|\varphi| + 1 = \text{Rank}(u)$. Define $\text{Elim}(u) = \text{Red}(\text{Elim}((u)_4), \text{Elim}((u)_5), \ulcorner \varphi \urcorner)$.

Case 2. $\text{Rule}(u) = \ulcorner \omega \urcorner$. Define $\text{Elim}(u) = \langle (u)_0, \dots, (u)_3, \ulcorner 2^{\xi_1} \urcorner, k, (u)_6, e' \rangle$ where $\ulcorner \xi^1 \urcorner = (u)_4$ and $e' = e'(e, u)$ is a code of $\text{Elim}([(u)_7](n))$ as a primitive recursive function of n ; e' as a function of e and u is primitive recursive. The other cases are treated similarly. By $<$ -induction on $|u|$ one can prove easily that $\text{Elim}(u)$ has the required properties. $\square$

4.2.5. Now we prove Theorem 4.2, following the sketch in 4.2.1. So let a $\mathbf{Z}$ -derivation of $\exists m \varphi(n, m)$ be given and let u be a code of the corresponding $\mathbf{Z}_\infty$ -derivation (cf. 4.2.3). Hence $|u| = \ulcorner \xi \urcorner < \ulcorner \omega \cdot 2 \urcorner$. By a finite number of applications of the Cut-Elimination Theorem in 4.2.4 we obtain a code u^* of a cut-free $\mathbf{Z}_\infty$ -derivation of $\exists m \varphi(n, m)$ with $|u^*| \leq \ulcorner 2^{\xi}_{\text{Rank}(u)} \urcorner$. Then $\text{Sub}(u^*, \ulcorner n^1 \urcorner, \ulcorner \bar{t}^1 \urcorner)$ is a code for a cut-free $\mathbf{Z}_\infty$ -derivation of $\exists m \varphi(\bar{t}, m)$. We may assume $\text{Var}(\text{Sub}(u^*, \ulcorner n^1 \urcorner, \ulcorner \bar{t}^1 \urcorner)) = \emptyset^*$ (otherwise apply $\text{Sub}(\cdot, \ulcorner m^1 \urcorner, \ulcorner 0 \urcorner)$ for any $m \in \text{Var}(\text{Sub}(u^*, \ulcorner n^1 \urcorner, \ulcorner \bar{t}^1 \urcorner))$). Hence the $\mathbf{Z}_\infty$ -derivation coded by $\text{Sub}(u^*, \ulcorner n^1 \urcorner, \ulcorner \bar{t}^1 \urcorner)$ contains only improper instances of the ω -rule, which may be cancelled. However, the function F_0 corresponding for codes to this cancellation is not primitive recursive, but only $< \varepsilon_0$ -recursive: in case $\text{Rule}(v) = \ulcorner \omega \urcorner$ we have to define $F_0(v) = F_0([(v)_6](0))$ and we only know $([(v)_6](0)) < |v|$. Now from $F_0(\text{Sub}(u^*, \ulcorner n^1 \urcorner, \ulcorner \bar{t}^1 \urcorner))$ we can easily read off primitive recursively all (closed) terms $s_0, \dots, s_{k-1}$ used in instances of the rule $\exists$ in the corresponding derivation. Since by the same argument as in the proof of Herbrand's Theorem 2.9 we get a derivation of $\varphi(\bar{t}, s_0), \dots, \varphi(\bar{t}, s_{k-1})$, we know that at least one $\varphi(\bar{t}, s_i)$ must be true. Let $F(i)$ be the least numerical value of some s_j such that $\varphi(\bar{t}, s_j)$ is true. This completes the proof of Theorem 4.2. $\square$

4.3. We now turn to a generalization of Theorem 4.2 to arbitrary $\mathbf{Z}$ -formulas. For the formulation of the result we need the notion of the *Herbrand normal form* φ_H of a formula φ , which we introduce first.

The general definition of φ_H is sufficiently explained by the following example. Let $\varphi \equiv \exists n \forall m \exists k \forall p \psi(n, m, k, p)$. Then $\varphi_H \equiv \exists n, k \psi(n, f(n), k, g(n, k))$ with function variables f, g . One can show easily that $\varphi \rightarrow \varphi_H$ is derivable (logically and hence) in $\mathbf{Z}$, and furthermore that if φ_H is derivable in $\mathbf{Z}$ then so is φ (cf. SHOENFIELD [1967]).

In general, for an arbitrary prenex formula φ the Herbrand normal form φ_H is obtained from φ by (i) dropping all universal quantifiers in the prefix of φ , and (ii) replacing any variable m bound by a universal quantifier in φ by $f(\mathbf{n})$, where $\mathbf{n}$ are all variables preceding m in the prefix of φ and bound by existential quantifiers, and f is a new function variable. Hence φ_H has the form $\exists \mathbf{m} \varphi^H$ with φ^H quantifier-free and generally containing new function variables. Again $\varphi \rightarrow \varphi_H$ is derivable (logically and hence) in $\mathbf{Z}$, and if φ_H is derivable in $\mathbf{Z}$ then so is φ .

4.4. THEOREM (KREISEL [1952]). *Let φ be a formula without set variables derivable in $\mathbf{Z}$. Let $\varphi_H \equiv \exists \mathbf{m} \varphi^H(f, \mathbf{n}, m)$ be its Herbrand normal form. Then*

we can find $< \varepsilon_0$ -recursive functionals G such that for all functions F and numbers i , $\varphi^H(F, i, G(F, i))$ holds.

PROOF. For simplicity assume $\varphi_H \equiv \exists m \varphi^H(f, n, m)$ with φ^H quantifier-free and without free variables other than those shown. Since by assumption φ is derivable in $\mathbf{Z}$, we know that also φ_H is derivable in $\mathbf{Z}$. We have to construct a function $G \in \text{Rec}_{<\varepsilon_0}$ such that for any function F and number i , $\varphi^H(F, i, G(F, i))$ holds.

The proof is completely parallel to the proof of Theorem 4.2; we only have to relativize it to a given function F .

We first introduce a relativization $\mathbf{Z}_\infty(F)$ of $\mathbf{Z}_\infty$. The language of $\mathbf{Z}_\infty(F)$ is the language of $\mathbf{Z}$ without set variables and with just one distinguished function variable f . A finite set Δ of formulas is called a $\mathbf{Z}_\infty(F)$ -axiom if Δ consists of atomic or negated atomic formulas without number variables such that $\forall \Delta$ is a tautological consequence of substitution instances of the quantifier-free axioms of $\mathbf{Z}$ and the additional axioms $f(\bar{j}) = \bar{k}$ for all j, k such that $F(j) = k$. The rules of $\mathbf{Z}_\infty(F)$ are the same as the rules for $\mathbf{Z}_\infty$.

The treatment of cut-elimination for $\mathbf{Z}_\infty$ in Section 3.4 carries over nearly unchanged to $\mathbf{Z}_\infty(F)$. Just note, for the Evaluation Lemma, that any term $s(f)$ without number variables has a numerical value i under the assignment $f \mapsto F$, and $s(f) = \bar{i}$ is a $\mathbf{Z}_\infty(F)$ -axiom. Now the proof of Theorem 4.2 can be adapted almost word for word, with the following exceptions.

(1) In the definition of codes for $\mathbf{Z}_\infty(F)$ -derivations we replace $[e](i)$ by $[e](F, i)$; $[e]$ is now the e -th primitive recursive functional (in the sense of Kleene).

(2) The functions Weak, Eval, Sub, Inv_i, Inv, Red, Elim, F_0 are to be replaced by functionals with F as an additional argument. This completes the proof of Theorem 4.4. $\square$

4.5. We now state a converse to Theorem 4.4 (and hence also to Theorem 4.2) and sketch its proof.

THEOREM. *Let F be a $< \varepsilon_0$ -recursive functional. Then F can be introduced in a recursive extension of $\mathbf{Z}$.*

4.5.1. For the proof we need an auxiliary notion: the *modulus of continuity* of a functional F . We now introduce this notion.

First note that any $< \varepsilon_0$ -recursive functional $F(\mathbf{n}, \mathbf{f})$ is continuous in the sense that it depends only on a finite part of any of its function arguments. Or equivalently, F is continuous for the discrete topology of $\mathbf{N}$ and the

corresponding product topology on product spaces. This can be seen easily by induction over the build-up of $< \varepsilon_0$ -recursive functionals. A functional M_F is called a modulus of continuity for F iff for any $\mathbf{n}, \mathbf{f}$, $M_F(\mathbf{n}, \mathbf{f})$ codes a finite set S of natural numbers such that for any two tuples of functions $\mathbf{f}$ and $\mathbf{f}'$ coinciding on $\bigcup_k S^k$ we have $F(\mathbf{n}, \mathbf{f}) = F(\mathbf{n}, \mathbf{f}')$.

4.5.2. We shall prove the following extension of Theorem 4.5.

THEOREM. *Let F be a $< \varepsilon_0$ -recursive functional. Then we can construct a $< \varepsilon_0$ -recursive modulus of continuity M_F for F , and F as well as M_F can be introduced in a recursive extension of $\mathbf{Z}$.*

Remark. The fact that any $< \varepsilon_0$ -recursive functional F has a $< \varepsilon_0$ -recursive modulus of continuity was first proved by Kreisel in lectures ('71/72); other proofs are in TROELSTRA [1973] and in SCHWICHTENBERG [1973].

The proof is by induction on the build-up of $< \varepsilon_0$ -recursive functionals. We only treat the case of α -recursion, the other cases being simpler or trivial. So let

$$F(\mathbf{n}, \mathbf{m}, \mathbf{f}) = G(\mathbf{n}, \mathbf{m}, (F \upharpoonright \mathbf{n})(\cdot, \mathbf{m}, \mathbf{f}), \mathbf{f}).$$

By the induction hypothesis we can assume that G and a modulus of continuity M_G of G have been introduced (in a recursive extension of $\mathbf{Z}$).

We first show how F can be introduced. The trick is not to introduce F directly, but via another functional which assigns to any argument $\mathbf{n}, \mathbf{m}, \mathbf{f}$ a *computation* u of F at this argument. Here u is called a computation of F at $\mathbf{n}, \mathbf{m}, \mathbf{f}$ iff the following holds.

(i) u is a finite function with domain $\{a_0, a_1, \dots, a_{k-1}\}$ where $a_0 < a_1 < \dots < a_{k-1} = n$.

(ii) $u(a_i) = G(a_i, \mathbf{m}, (u \upharpoonright a_i), \mathbf{f})$ for $i < k$, where $(u \upharpoonright a_i)$ is defined by

$$(u \upharpoonright a_i)(x) = \begin{cases} u(x) & \text{if } x = a_j \text{ for some } j < i, \\ 0 & \text{otherwise.} \end{cases}$$

(iii) $M_G(a_i, \mathbf{m}, (u \upharpoonright a_i), \mathbf{f}) \cap \{x \mid x < a_i\} \subseteq \{a_0, \dots, a_{i-1}\}$ for $i < k$. Note that any of the conditions (i)–(iii) is quantifier-free and does not involve F . Now one can prove in $\mathbf{Z} \forall \mathbf{n}, \mathbf{m}, \mathbf{f} \exists u$ (u is a computation of F at $\mathbf{n}, \mathbf{m}, \mathbf{f}$), by α -induction on $\mathbf{n}$. To see this, observe that adding to $\mathbf{Z}$ the arithmetical axiom of choice and second-order logic (but no second-order instances of

the induction schema) gives a conservative extension of $\mathbf{Z}$; this can either be proved directly using the method indicated in Chapter D.4, 5.5.1, or else follows from the much stronger result in Chapter D.4, 8.7. Hence the corresponding functional giving u as a functional of n, m, f can be introduced, and from this F can be easily defined explicitly. Furthermore, from the conditions (i)–(iii) and the fact that M_G is a modulus of continuity for G one can prove (in $\mathbf{Z}$) the defining equations of F .

Now M_F can be defined from F by the following α -recursion

$$M_F(n, m, f) = S^* \cup^* \bigcup_{\substack{a < n \\ a \in S}}^* M_F(a, m, f),$$

where

$$S^* = M_G(n, m, (F \upharpoonright n)(\cdot, m, f), f).$$

Hence, by the argument just given, M_F too can be introduced. By α -induction on n one can show in $\mathbf{Z}$ that M_F is a modulus of continuity for F , using the defining equations for F and the fact that M_G is a modulus of continuity for G .

5. Transfinite induction and the reflection principle

5.1. We now consider $\mathbf{Z}$ without set and function variables. The (uniform) *reflection principle* for $\mathbf{Z}$ is the schema

$$\text{RP} \quad \text{Der}(x, \ulcorner \varphi(\dot{n}) \urcorner) \rightarrow \varphi(n)$$

where $\text{Der}(x, y)$ is the primitive recursive predicate which holds iff x codes a $\mathbf{Z}$ -derivation $d \vdash \varphi$ and $y = \ulcorner \varphi \urcorner$, and $\ulcorner \varphi(\dot{n}) \urcorner$ is a primitive recursive function of n and denotes a code for the formula obtained from $\varphi(n)$ by substituting the numerals $\dot{n}$ for the variables n , i.e., $\ulcorner \varphi(\dot{n}) \urcorner = \text{Subst}(\ulcorner \varphi(n) \urcorner, \ulcorner n \urcorner, \text{Num}(n))$ with the obvious primitive recursive functions Subst and Num . Furthermore, we assume that x is not free in $\varphi(n)$. Note that RP trivially implies the consistency of $\mathbf{Z}$, i.e. the formula $\forall x \neg \text{Der}(x, \ulcorner 0 = 1 \urcorner)$. The schema of transfinite induction up to ε_0 for $\mathbf{Z}$ is

$$\text{TI}_{\varepsilon_0} \quad \forall n (\forall m (m < n \rightarrow \varphi(m)) \rightarrow \varphi(n)) \rightarrow \forall n \varphi(n).$$

5.2. THEOREM (KREISEL and LÉVY [1968]). $\mathbf{Z}$ together with the schema RP is equivalent to $\mathbf{Z}$ together with the schema $\text{TI}_{\varepsilon_0}$.

PPROOF. We begin with the easy part and show that $\text{TI}_{\varepsilon_0}$ is derivable in $\mathbf{Z} + \text{RP}$. So let $\varphi(n)$ be given and define $\psi(k)$ to be

$$\forall n (\forall m (m < n \rightarrow \varphi(m)) \rightarrow \varphi(n)) \rightarrow \forall n (n < F(k) \rightarrow \varphi(n))$$

where $F(k) = \ulcorner \omega_k \urcorner$, $\omega_0 = 1$, $\omega_{i+1} = \omega^{\omega_i}$. Since $\mathbf{Z} \vdash \forall m \exists k m < F(k)$, it suffices to derive $\psi(k)$ in $\mathbf{Z} + \text{RP}$. Now from the proof of GENTZEN [1943] (or SCHÜTTE [1960]) of transfinite induction up to ω_k in $\mathbf{Z}$ one can extract a primitive recursive function G such that $\mathbf{Z} \vdash \forall k \text{Der}(G(k), \ulcorner \psi(\dot{k}) \urcorner)$. From this and RP we obtain $\psi(k)$, as required.

The proof of the converse will cover the rest of this section. We have to show that RP is derivable in $\mathbf{Z} + \text{TI}_{\varepsilon_0}$. So assume $\text{Der}(x, \varphi(\dot{n}))$. Now the following lemma is derivable in $\mathbf{Z}$ (cf. 4.2.3 and 5.2.2):

EMBEDDING LEMMA. *We have a primitive recursive function Emb such that for any x, y with $\text{Der}(x, y)$ the following holds.*

- (i) $\text{Emb}(x) =: u_x \in \text{Code}$,
- (ii) $\text{End}(u_x) = y$, and
- (iii) $|u_x| < \ulcorner \omega \cdot 2 \urcorner$.

Also the Cut-Elimination Theorem of 4.2.4 is derivable in $\mathbf{Z} + \text{TI}_{\varepsilon_0}$ (cf. 5.2.2). Hence we can prove in $\mathbf{Z} + \text{TI}_{\varepsilon_0}$ that we have a $u_x^* \in \text{Code}$ (depending primitive recursively on x) with $\text{End}(u_x^*) = \ulcorner \varphi(\dot{n}) \urcorner$ and $\text{Rank}(u_x^*) = 0$. In 5.2.1 we shall give within $\mathbf{Z}$ a *partial truth definition* Tr_q with the following characteristic property: For any formula $\psi(\mathbf{n})$ with depth of quantifier-nesting $\text{QD}(\psi(\mathbf{n})) \leq q$ one can prove in $\mathbf{Z}$

$$\text{Tr}_q(\ulcorner \psi(\dot{\mathbf{n}}) \urcorner) \leftrightarrow \psi(\mathbf{n}).$$

Now the following lemma obviously holds (use $<$ -induction on $|u|$) and is derivable in $\mathbf{Z} + \text{TI}_{\varepsilon_0}$ (cf. 5.2.2):

TRUTH LEMMA. *For any $u \in \text{Code}$ with $\text{Rank}(u) = 0$ and $\text{End}(u) = \ulcorner \psi \urcorner$ where $\text{QD}(\psi) \leq q$ we have $\text{Tr}_q(\ulcorner \psi \urcorner)$.*

Specializing this to $u = u_x^*$ we obtain $\text{Tr}_q(\ulcorner \varphi(\dot{\mathbf{n}}) \urcorner)$ and hence $\varphi(\mathbf{n})$, both in $\mathbf{Z} + \text{TI}_{\varepsilon_0}$.

5.2.1. We define for any $q \geq 0$ a set Tr_q which is intended to give a *partial truth definition* for all $\mathbf{Z}$ -formulas φ with depth of quantifier-nesting $\text{QD}(\varphi) \leq q$.

First note that we can easily introduce a function Val (in a recursive extension of $\mathbf{Z}$) such that for any term $s(\mathbf{n})$ $\text{Val}(\ulcorner s(\dot{\mathbf{n}}) \urcorner) = s(\mathbf{n})$ is derivable in $\mathbf{Z}$.

DEFINITION. Tr_q is defined as follows.

- (i) $\text{Tr}_q({}^l P s_0(\dot{n}) \cdots s_{p-1}(\dot{n})^l) \leftrightarrow P(\text{Val}({}^l s_0(\dot{n})^l), \dots, \text{Val}({}^l s_{p-1}(\dot{n})^l))$ for any predicate or set symbol P .
- (ii) $\text{Tr}_q({}^l \varphi_0 \wedge \varphi_1^l) \leftrightarrow \text{Tr}_q({}^l \varphi_0^l) \wedge \text{Tr}_q({}^l \varphi_1^l)$ if $\text{QD}(\varphi_i) \leq q$. Similarly for $\vee$.
- (iii) $\text{Tr}_q({}^l \forall n \varphi(n)^l) \leftrightarrow \forall n \text{Tr}_{q-1}({}^l \varphi(\dot{n})^l)$ if $q \geq 1$ and $\text{QD}(\varphi(n)) \leq q - 1$. Similarly for $\exists$.

LEMMA. $\text{Tr}_q({}^l \varphi(\dot{n})^l) \leftrightarrow \varphi(n)$ is derivable in $\mathbf{Z}$ if $\text{QD}(\varphi(n)) \leq q$.

The proof is obvious, using induction on $|\varphi(n)|$.

5.2.2. We now show that the Embedding Lemma and the Truth Lemma stated in Section 5.2 as well as all the lemmas in 4.2.4 up to and including the Cut-Elimination Theorem are derivable in $\mathbf{Z} + \text{TI}_{\varepsilon_0}$. The only point to verify is that all these lemmas can be formulated in the language of $\mathbf{Z}$; the formalization of the proofs is then routine. Now the only possible obstacle against such a formulation is the occurrence of the inductively defined notion of a code for a $\mathbf{Z}_\infty$ -derivation (cf. 4.2.2) in all these lemmas. We now show how this notion can be represented in purely generalized form.

Infinite $\mathbf{Z}_\infty$ -derivations may be considered as well-founded trees, where at each node there is either no branching at all (i.e. it is a bottommost node) and an instance of the rule A is affixed, or there is a 1-fold branching (corresponding to the rules $\vee_i, \forall \exists$), or a 2-fold branching (corresponding to the rules $\wedge$, Cut), or an ω -fold branching (corresponding to the ω -rule). Then any code u of a $\mathbf{Z}_\infty$ -derivation d can be thought of as obtained inductively by affixing to each node of the tree corresponding to d a code of the corresponding subderivation. Hence the property $u \in \text{Code}$ is equivalent to u having such a well-founded genealogic tree. But the latter fact can be easily written in purely generalized form: One has to express that at any node (= sequence number) n the tree is locally correct, i.e. that the code u_n affixed there (u_n can be easily defined by induction on n) and all its predecessors $u_{n \cdot (i)}$, $i = 0, 1, 2, \dots$, fulfill a relation as given in the definition of codes for $\mathbf{Z}_\infty$ -derivations. The well-foundedness is then obtained automatically, since in particular $|u_{n \cdot (i)}| < |u|$ is required and $<$ is a well-ordering. $\square$

References

- BACHMANN, H.
 [1955] *Transfinite Zahlen* (Springer, Berlin).

GENTZEN, G.

- [1943] Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie, *Math. Ann.*, **119**, 140–161.

GÖDEL, K.

- [1958] Über eine bisher noch nicht benützte Erweiterung des finiten Standpunkts, *Dialectica*, **12**, 280–287.

HILBERT, D. and BERNAYS, P.

- [1934] *Grundlagen der Mathematik*, I (Springer, Berlin).

KLEENE, S.C.

- [1958] Extension of an effectively generated class of functions by enumeration, *Colloq. Math.*, **7**, 67–78.
 [1959] Recursive functionals and quantifiers of finite type I, *Trans. Am. Math. Soc.*, **91**, 1–52.

KREISEL, G.

- [1952] On the interpretation of non-finitist proofs II, *J. Symbolic Logic*, **17**, 43–58.
 [1958] Mathematical significance of consistency proofs, *J. Symbolic Logic*, **23**, 155–182.
 [1968] A survey of proof theory, *J. Symbolic Logic*, **33**, 321–388.

KREISEL, G. and LÉVY, A.

- [1968] Reflection principles and their use for establishing the complexity of axiomatic systems, *Z. Math. Logik Grundlagen Math.*, **14**, 97–142.

SCHÜTTE, K.

- [1960] *Beweistheorie* (Springer, Berlin).

SCHWICHTENBERG, H.

- [1973] Einige Anwendungen von unendlichen Termen und Wertfunktionalen (Habilitationsschrift, Münster).
 [1975] Elimination of higher type levels in definitions of primitive recursive functionals by means of transfinite recursion, in: *Logic Colloquium '73*, edited by H. E. Rose and J. C. Shepherdson (North-Holland, Amsterdam), pp. 279–303.

SHOENFIELD, J.R.

- [1967] *Mathematical Logic* (Addison-Wesley, New York).

TAIT, W.W.

- [1968] Normal derivability in classical logic, in: *The Syntax and Semantics of Infinitary Languages*, edited by J. Barwise (Springer, Berlin), pp. 204–236.

TROELSTRA, A.S., editor

- [1973] *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*, Lecture Notes in Mathematics, Vol. 344 (Springer, Berlin).

Herbrand's Theorem and Gentzen's Notion of a Direct Proof

RICHARD STATMAN

Contents

1. Introduction .	898
2. Preliminaries . . .	901
3. Direct computations	904
4. Conclusion	910
References	912

1. Introduction

1.1. To explain the results and methods characteristic of the theory of proofs we reconsider here a special case of the following corollary to the Completeness Theorem.

THEOREM. *If $G(x_1, \dots, x_n)$ is a quantifier-free formula of predicate logic and $\exists x_1 \cdots x_n G(x_1, \dots, x_n)$ is valid, then there are terms t_j^i , for $1 \leq i \leq m$ and $1 \leq j \leq n$, such that $\forall_{1 \leq i \leq m} G(t_1^i, \dots, t_n^i)$ is valid.*

This result is known in the literature as Herbrand's Theorem; see e.g. Theorem 2.9 of Chapter D.2.

1.2. There is a recursive method of passing from any derivation of $\exists x_1 \cdots x_n G(x_1, \dots, x_n)$ in the predicate calculus to the list of terms and a derivation of $\forall_{1 \leq i \leq m} G(t_1^i, \dots, t_n^i)$. The existence of this method, and of a partial recursive one independent of the derivation, follows from the soundness and completeness of the rules. The non-existence of a recursive method depending only on the formula follows from the recursive undecidability of validity.

1.3. The theory of proofs uses these general observations for orientation and makes the following types of distinctions in order to get more rewarding results:

(i) Not arbitrary quantifier-free G are considered but rather certain subclasses. For example, in the language of semi-groups, we pick out those formulae which naturally express that two words (terms) are equal in a certain finitely generated, finitely presented cancellation semi-group. More generally, if $A_1, \dots, A_p$ are fixed prime formulae, and $I_1, \dots, I_q$ fixed implicational formulae with $I_j = P_1^j \rightarrow (\cdots (P_{l(j)}^j \rightarrow C^j) \cdots)$ for P_i^j and C^j prime, we consider the collection L of formulae G of the form $(\bigwedge_{1 \leq i \leq p} A_i \wedge \bigwedge_{1 \leq j \leq q} I_j \wedge \bigwedge_{1 \leq k \leq m} B_k) \rightarrow B_{m+1}$ for B_i prime and not containing $x_1 \cdots x_n$.

(ii) Not arbitrary sound complete rules are considered but rather rules adapted to the mathematical content of L . In the above example, for relations $R_1 \cdots R_m$, if $w_1 = w_2$ then $w_1 = w_2$ is derivable from $R_1 \cdots R_m$, the associativity axioms $((ab)c) = (a(bc))$, and the identity axioms $a = a$ by the rule of substituting equals for equals together with the cancellation laws

$$\frac{(ab) = (ac)}{b = c} \quad \text{and} \quad \frac{(ba) = (ca)}{b = c}.$$

More generally, if $\exists x_1 \cdots x_n G(x_1, \dots, x_n)$ is valid, for G in L , then B_{m+1} is derivable from $B_1 \cdots B_m$ together with the axioms θA_i for each substitution θ for $x_1 \cdots x_n$, by the rules

$$\frac{\theta P_1^i \cdots \theta P_{r(i)}^i}{\theta C^i}$$

for each substitution θ for $x_1 \cdots x_n$ (this is a simple consequence of Gentzen's Cut-Elimination Theorem).

(iii) Not only the complexity of the terms t_i^j is considered but also how the length of a derivation is related to the choice of the corresponding t_i^j . In particular, the following questions are raised:

(a) Which substitutions θ are needed to derive B_{m+1} from $B_1 \cdots B_m$?

(b) How is the length of a derivation of B_{m+1} from $B_1 \cdots B_m$ related to the complexity of the corresponding θ 's?

(c) What is an efficient order of application of the rules?

It should be noted that (a), (b) and (c) are by no means trivial even if validity of formulae in L is recursively decidable; proof-theoretic methods are used to study the efficiency of decision procedures.

1.4. A principal aim of the theory of proofs is to make differences among proofs, previously judged only by "aesthetic criteria of elegance or convenience", objects of study. One such difference, which has received a great deal of attention, involves "directness" where for our purposes a direct proof is one which contains no term more complicated than all those in the theorem proved. If direct proofs are formalizable in the above system of rules for L then this fact already provides an answer to question (a). In particular, such direct proofs may be the values of a complete proof-search procedure of a kind similar to the so-called semantic tableaux.

In 1961 Kreisel and Tait gave an equation calculus intended to formalize the notion of a computation from equations which define the values of a number-theoretic function. This calculus K is related in the manner sketched above to a set J of axioms (for an elegant formulation see KREISEL and KRIVINE [1967], Exercise 8, p. 48), and, using this relation, Kreisel and Tait showed that K is complete in the sense that, for equations E_i , if $(E_1 \wedge \cdots \wedge E_m) \rightarrow E_{m+1}$ is valid then E_{m+1} is derivable from $E_1 \cdots E_m$. We shall try to answer questions (a), (b) and (c) for K ; one thing we will prove is that direct "computations" are formalizable in K .

1.5. Kreisel and Tait actually gave two proofs of completeness, both of which are instructive. The first proof is the above-mentioned model-

theoretic one; consider the two-sorted first-order language corresponding to the structures $\langle \mathbb{N}, F, =, 0, s \rangle$, where $\mathbb{N}$ is the set of natural numbers, and F is a collection of number-theoretic functions containing the function constantly 0, the successor function s , and closed under explicit definition (lambda-abstraction). Let J be the following collection of axioms:

- (1) $x = x$,
- (2) $(fx = gx \wedge x = y) \rightarrow fy = gy$,
- (3) $(fx = gx \wedge y = x) \rightarrow fy = gy$,
- (4) $sx = sy \rightarrow x = y$,
- (5) $0 = sx \rightarrow y = z$,
- (6_n) $x = s^n x \rightarrow y = z$,

where $s^1 = s$ and $s^{k+1} = ss^k$. The members of J are clearly valid over the collection of structures $\langle \mathbb{N}, F, =, 0, s \rangle$. In addition, if one considers general models of J , if $(E_1 \wedge \cdots \wedge E_m) \rightarrow E_{m+1}$ is not valid, then it has a counter-model of the form $\langle \mathbb{N}, F, =, 0, s \rangle$. In particular, the function variables in the E_i can be interpreted as number-theoretic functions with finite support; thus, we have decidability as well as completeness for K .

1.6. The second proof goes by way of formalizing in K a particularly elementary decision procedure for the validity of $(E_1 \wedge \cdots \wedge E_m) \rightarrow E_{m+1}$. This formalization results in a complete proof-search procedure, and analysis of the proof provides answers to questions (a) and (c), namely,

(a) if $(E_1 \wedge \cdots \wedge E_m) \rightarrow E_{m+1}$ is valid and $E_1 \wedge \cdots \wedge E_m$ is satisfiable, then there is a direct computation of E_{m+1} from $E_1 \cdots E_m$ of length $\leq 2^{kp}$, where p is the number of occurrences of non-logical symbols in $(E_1 \wedge \cdots \wedge E_m) \rightarrow E_{m+1}$ (if $E_1 \wedge \cdots \wedge E_m$ is not satisfiable, then a similar result is true, but not necessarily for E_{m+1}), and

(c) the validity of $(E_1 \wedge \cdots \wedge E_m) \rightarrow E_{m+1}$ can be decided by a deterministic Turing machine in polynomial time (a polynomial number of operations in the length of a code of the formula).

Here it should be noted that the bound 2^{kp} is for computations as trees of equation occurrences; by identifying different occurrences of the same equation, these can be coded as sequences of equations with a resulting bound of kp^2 .

We present the second proof of Kreisel and Tait.

1.7. In order to give an answer to question (b) we will analyze computations in K in a manner similar to Gentzen's cut-elimination argument. In particular, we will show that if the individual inferences of a given

computation are “fully analyzed”, then these inferences can be permuted so as to obtain a direct computation. More precisely, we will prove that

(b) if in a computation T of E_{m+1} from $E_1 \cdots E_m$

(i) the rules corresponding to the axioms (5) and (6_n) are not used at all, and

(ii) each application of the rule of substituting equals for equals (corresponding to axioms (2) and (3)) substitutes for at most one occurrence of one of the equals,

then there is a direct computation of E_{m+1} from $E_1 \cdots E_m$ of length $\leq kp^2$, where p is the length of T

2. Preliminaries

2.1. We consider equations E between individual terms $a, b, c, \dots$, possibly containing function variables, and finite sets of equations S .

2.2. NOTATION. We write $[\cdots](a_1/x_1, \dots, a_n/x_n)$ for the operation of simultaneously substituting a_i for x_i in $[\cdots]$; substitutions θ may substitute function terms $\lambda x_1 \cdots x_n a$ for n -place function variables f under the definitions $\theta(fa_1 \cdots a_n) = (\theta f)(\theta a_1) \cdots (\theta a_n)$ and $(\lambda x_1 \cdots x_n a)b_1 \cdots b_n = a(b_1/x_1, \dots, b_n/x_n)$.

2.3. DEFINITION. A function M from terms to non-negative integers is called a *measure* if $M(a) \leq M(b) \Rightarrow M(c(a/x)) \leq M(c(b/x))$ and, whenever x occurs in c , $M(a) \leq M(c(a/x))$.

If M is a measure we set $M(a = b) =_{\text{df}} M(a) + M(b)$, and $M(S) =_{\text{df}} \sum_{E \in S} M(E)$.

Length is a measure, where $\text{lh}(a) =_{\text{df}}$ the number of occurrences of symbols in a .

2.4. DEFINITION. A substitution θ is called *non-projecting* if whenever $\theta f = \lambda x_1 \cdots x_n a$ each x_i actually occurs in a .

Note that if M is a measure and θ is non-projecting, then the function M^* defined by $M^*(a) = M(\theta a)$ is a measure.

2.5. DEFINITION. S is called *simple* if each equation in S has one of the forms $x = 0$, $x_1 = x_2$, $x_1 = sx_2$, or $x_{m+1} = fx_1 \cdots x_m$.

2.6. DEFINITION. The calculus K of Kreisel and Tait consists of the axioms $a = a$ and the rule of substituting equals for equals

$$(1) \quad \frac{E(a/x) \quad a \doteq b}{E(b/x)},$$

where $a \doteq b$ is, ambiguously, $a = b$ and $b = a$, together with the rules

$$(2) \quad \frac{sa = sb}{a = b},$$

$$(3) \quad \frac{0 = sa}{b = c},$$

$$(4_n) \quad \frac{a = s^n a}{b = c}$$

The calculus consisting of the rule (1) only will be called H (and corresponds to axioms (1), (2) and (3) of J).

2.7. DEFINITION. *Computations* T in K or H are binary trees of equation occurrences built up from assumptions and axioms according to the rules; it should be clear what it means for T to be a K or H computation of E from S .

2.8. DEFINITION. The *length* of a computation T is the number of occurrences of equations in T .

2.8. DEFINITION. T is called *singular* if each of its inferences of the form (1) has x occurring exactly once in E .

2.10. DEFINITION. Given a computation T , a *switch* is a replacement of a subcomputation

$$\frac{\frac{T_1 \quad T_2}{E(a/x, b/y) \quad a \doteq c} \quad T_3}{\frac{E(c/x, b/y) \quad b \doteq d}{E(c/x, d/y)}} \quad \text{by} \quad \frac{\frac{T_1 \quad T_3}{E(a/x, b/y) \quad b \doteq d} \quad T_2}{\frac{E(a/x, d/y) \quad a \doteq c}{E(c/x, d/y)}}$$

and a *shift* is a replacement of a subcomputation

$$\frac{\frac{T_1 \quad T_2}{E(a/x) \quad a \doteq c(b/y)} \quad T_3}{\frac{E(c(b/y)/x) \quad b \doteq d}{E(c(d/y)/x)}} \quad \text{by} \quad \frac{T_1 \quad \frac{T_2 \quad T_3}{a \doteq c(b/y) \quad b \doteq d}}{\frac{E(a/x) \quad a \doteq c(d/y)}{E(c(d/y)/x)}}$$

or

$$\frac{\frac{T_1}{E(b(a/x)/y)} \quad \frac{T_2}{a \doteq c}}{E(b(c/x)/y)} \quad \frac{T_3}{b(c/x) \doteq d} \quad \text{by} \quad \frac{\frac{T_1}{E(b(a/x)/y)} \quad \frac{\frac{T_3}{b(c/x) \doteq d} \quad \frac{T_2}{c \doteq a}}{b(a/x) \doteq d}}{E(d/y)}.$$

A *move* is a switch or a shift, and we say that T_1 *reduces* to T_2 if T_2 results from T_1 by a sequence of moves.

2.11. Note that if T_1 is singular, and T_1 reduces to T_2 or T_2 reduces to T_1 , then

- (i) T_2 is singular, and in addition,
- (ii) each combination of two inferences in T_1 nested to the left is covered by a clause in the definition of a move, and
- (iii) each combination of two inferences in T_1 nested to the right arises from some clause in the definition of shift.

Further observe that if T is singular then:

- (a) there is a T_R such that T reduces to T_R and each sequence of moves beginning with T_R is a sequence of switches, and
- (b) there is a T_L such that T_L reduces to T and each sequences of moves ending in T_L is a sequence of switches.

This can be seen by measuring the “leftness” of T by the n -tuple $(k_1, \dots, k_n)$, where k_i is the length of the i -th maximal path, from left to right, in T , and ordering these lexicographically. A sequence of switches followed by a shift, all involving inferences “on” the leftmost path of a subcomputation of T , always decreases leftness. T_R can be obtained by iterating this procedure as often as possible. T_L can be obtained by reversing it, less switches, as often as possible.

2.12. If T is a singular H computation then each subcomputation of T_R has the form

$$\frac{\frac{T_1}{E(a_1/x_1, \dots, a_n/x_n)} \quad a_1 \doteq b_1}{E(b_1/x_1, \dots, a_n/x_n)} \quad \dots \quad \frac{\frac{T_n}{E(b_1/x_1, \dots, a_n/x_n)} \quad a_n \doteq b_n}{E(b_1/x_1, \dots, b_n/x_n)}$$

and T_L has the form

$$\frac{E_1 \quad E_2}{E_3} \quad \dots \quad \frac{E_n \quad E_{n+1}}{E_{n+2}}.$$

If T is a singular K computation, then this applies equally well to the maximal fragments of T_R and T_L which are H computations; these maximal fragments are called H fragments.

2.13. DEFINITION. If M is a measure, we say that a computation T of E from S is M -direct if for each term b occurring in T there is a term c occurring in E or S with $M(b) \leq M(c)$.

2.14. CONVENTION. Individual variables are interpreted as ranging over the set of natural numbers, function variables as ranging over number-theoretic functions, and 0 and s as denoting zero and the successor function, respectively.

2.15. DEFINITION. $\wedge S \rightarrow E$ is said to be *analytic* if it is valid and $\wedge S$ is satisfiable.

Of course, if $\wedge S$ is not satisfiable there is no reason to expect lh-direct computations from S to exist for all E , but rather only for some instance of the premiss of (3) or (4_n). Take, for example,

$$S_n =_{\text{df}} \{x_1 = sx_n, x_2 = sx_1, \dots, x_n = sx_{n-1}\} \quad \text{and} \quad E =_{\text{df}} 0 = s0.$$

With this in mind, we will restrict our attention to K less the rules (3) and (4_n) continuing to call this K . K is complete in the sense that if $\wedge S \rightarrow E$ is analytic, then E is derivable from S .

3. Direct computations

3.1. PROPOSITION. Suppose that S is simple and M is a measure; then

(i) if $\wedge S \rightarrow x = y$ is analytic, then there is an M -direct computation of $x = y$ from S of length $\leq 2^{3k}$, where k is the number of variables occurring in S , and

(ii) if $\wedge S$ is not satisfiable, then there is an M -direct computation of $x = s^p x$ ($0 = sx$) from S of length $\leq 2^{4k}$, where $p \leq \text{card}(S)$, k is the number of variables occurring in S , and x occurs in S .

PROOF. We proceed inductively, constructing at stage n a collection C_n of computations of members of S_n from S , and a computation T_n . The members of C_n are used as auxiliaries in constructing T_{n+1} which has the form

$$\begin{array}{c} x_1 = y_1 \frac{T_1^*}{x_2 = y_2} \cdot \\ \vdots \\ x_n = y_n \frac{T_n^*}{x_{n+1} = y_{n+1}} \end{array}$$

where each T_i^* is a computation from S . The construction must stop at some $n_0 \leq$ the number of variables occurring in S .

Stage 1: Set $S_1 =_{\text{df}} S \cup \{x = x : x \text{ occurs in } S\}$, $C_1 =_{\text{df}} S_1$, $x_1 =_{\text{df}} x$, $y_1 =_{\text{df}} y$, and $T_1 =_{\text{df}} x = y$.

Stage $n+1$: Case 1. There are $a = c$ and $b = c$ in S_n such that a is not b and $M(a) \leq M(b)$. Select computations T_a and T_b of $a = c$ and $b = c$, resp., from C_n ; set $S_{n+1} =_{\text{df}} S_n (a/b)$, $x_{n+1} =_{\text{df}} x_n (a/b)$, $y_{n+1} =_{\text{df}} y_n (a/b)$,

$$T_n^* =_{\text{df}} \frac{T_b}{b = a} \frac{T_a}{b = a},$$

$$C_{n+1} =_{\text{df}} \left\{ \frac{T}{E(a/b)} \frac{T_n^*}{b = a} : T \text{ is a computation of } E \text{ from } S \text{ in } C_n \right\}$$

and

$$T_{n+1} =_{\text{df}} \frac{T_n}{x_{n+1} = y_{n+1}} \frac{T_n^*}{b = a}.$$

Case 2. Not case 1 but there are $c = sa$ and $c = sb$ in S_n such that a is not b and $M(a) \leq M(b)$. Select computations T_a and T_b of $c = sa$ and $c = sb$, resp., from C_n ; set $S_{n+1} =_{\text{df}} S_n (a/b)$, $x_{n+1} =_{\text{df}} x_n (a/b)$, $y_{n+1} =_{\text{df}} y_n (a/b)$,

$$T_n^* =_{\text{df}} \frac{T_a}{sb = sa} \frac{T_b}{b = a},$$

$$C_{n+1} =_{\text{df}} \left\{ \frac{T}{E(a/b)} \frac{T_n^*}{b = a} : T \text{ is a computation of } E \text{ from } S \text{ in } C_n \right\}$$

and

$$T_{n+1} =_{\text{df}} \frac{T_n}{x_{n+1} = y_{n+1}} \frac{T_n^*}{b = a}.$$

First suppose that $\wedge S \rightarrow x = y$ is analytic, then S_{n_0} has the following properties:

(i) If $fx_1 \cdots x_m$ occurs in S_{n_0} , then there is exactly one z such that $z = fx_1 \cdots x_m$ belongs to S_{n_0} .

(ii) If sz_1 occurs in S_{n_0} , then there is exactly one z such that $z = sz_1$ belongs to S_{n_0} .

(iii) If 0 occurs in S_{n_0} , then there is exactly one z such that $z = 0$ belongs to S_{n_0} .

(iv) If $z_1 = z_2$ belongs to S_{n_0} , then z_1 is z_2 .

(v) If $z = sz_1$ and $z = sz_2$ belong to S_{n_0} , then z_1 is z_2 .

(vi) There are no z_1 and z_2 such that $z_1 = sz_2$ and $z_1 = 0$ belong to S_{n_0} .

(vii) There are no $z_1 \cdots z_m$ such that $z_1 = sz_m$, $z_2 = sz_1, \dots, z_m = sz_{m-1}$ belong to S_{n_0} .

Thus an interpretation satisfying S_{n_0} can be read off from S_{n_0} and expanded to an interpretation satisfying S ; in particular, this interpretation does not satisfy $x_{n_0} = y_{n_0}$ unless x_{n_0} is y_{n_0} . Now it can easily be seen from the structure of T_{n_0} that $\wedge S \rightarrow (x_1 = y_1 \leftrightarrow x_{n_0} = y_{n_0})$, hence x_{n_0} is y_{n_0} . So we may take

$$\frac{x_{n_0} = y_{n_0} \quad T_{n_0}^*}{x_{n_0-1} = y_{n_0-1}} \\ \vdots \\ \frac{x_2 = y_2 \quad T_1^*}{x_1 = y_1}$$

for the desired M -direct computation of $x = y$ from S ; its length is $\leq 2^{3k}$, where k is the number of variables occurring in S , since the maximum length of a path in T_1^* is $\leq 3i$.

Now suppose that $\wedge S$ is not satisfiable, then, since S_{n_0} satisfies (i) to (v), either (vi) (with z_1 different from z_2) or (vii) fails. In the former case the desired computation is obvious. In the latter case, choose z_1 so that $M(z_i)$ is maximum, then for each $q \leq m$ we have $M(s^q z_j) = (M(s^m z_i))$, and a suitable computation of $z_i = s^m z_i$ from S can easily be constructed from those in C_{n_0} . $\square$

3.2. PROPOSITION. If M is a measure, then

(i) if $\wedge S \rightarrow a = b$ is analytic there is an M -direct computation of $a = b$ from S of length $\leq 2^{9(\text{lh}(S) + \text{lh}(a=b))}$, and

(ii) if $\wedge S$ is not satisfiable there is an M -direct computation of $a = s^p a$ ($0 = sa$) from S of length $\leq 2^{12 \text{lh}(S)}$, where $p \leq \text{lh}(S)$ and a occurs in S .

PROOF. (ii) is just like (i) using the corresponding case of Proposition 3.1, so we only do (i). To each occurrence t of a term in $\wedge S \rightarrow a = b$ assign a new variable x_t ; let

$$S_1 =_{\text{df}} \{x_{t_1} = 0, x_{t_2} = y, x_{st_3} = sx_{t_3}, x_{ft_4 \cdots t_m} = fx_{t_4} \cdots x_{t_m} : t_1 \text{ an occurrence of } 0, t_2 \text{ an occurrence of } y, st_3 \text{ and } ft_4 \cdots t_m \text{ occurrences}\}$$

and set

$$S_2 =_{\text{df}} \{x_{t_1} = x_{t_2}: t_1 = t_2 \text{ belongs to } S\}.$$

Now apply proposition to $\wedge (S_1 \cup S_2) \rightarrow x_a = x_b$ for the measure M^* defined by $M^*(c) = M(c(\dots, t/x_t, \dots))$. $\square$

3.3.1. DEFINITION. We say that a computation T of E from S has the *weak subterm property* if each inference in T of the form (2) has sa and sb occurring in S . T has the *subterm property* if it has the weak subterm property and each of its axioms $a = a$ has a occurring in E or S . Singular computations with the subterm property are related to M -direct ones by reducibility.

3.3.2. PROPOSITION. *If M is a measure and T is a singular computation with the subterm property, then T reduces to an M -direct T_M .*

PROOF. By applying a sequence of switches to T_R construct a T_M so that it contains no subcomputation of the form

$$\frac{\frac{T_1}{E(a/x, c/y)} \quad \frac{T_2}{a \doteq b}}{\frac{E(b/x, c/y)}{E(b/x, d/y)}} \quad \frac{T_3}{c \doteq d}$$

with $M(a) < M(b)$ and $M(d) \leq M(c)$. Since T_M is singular with the subterm property, it follows easily by induction over T_M that it is M -direct. $\square$

3.4. PROPOSITION. *If T is a singular computation of E from S with the weak subterm property, then there is a singular computation T_S of E from S with the subterm property of length $\leq \text{lh}(T)$.*

PROOF. Construct from T_L , by a sequence of switches, a computation containing no H fragment with an inference of the form

$$\frac{a_1 = b_1(c_1/x_1) \quad c_1 \doteq d_1}{a_1 = b_1(d_1/x_1)}$$

preceding one of the form

$$\frac{a_2(c_2/x_2) = b_2 \quad c_2 \doteq d_2}{a_2(d_2/x_2) = b_2}.$$

Each H fragment of this computation has the form

$$\begin{array}{c}
\frac{a_p = b_q \quad E_1}{a_{p-1} = b_q} \\
\vdots \\
\frac{a_2 = b_q \quad E_{p-1}}{a_1 = b_q \quad E_p} \\
\frac{a_1 = b_{q-1}}{a_1 = b_{q-1}} \\
\vdots \\
\frac{a_1 = b_2 \quad E_{p+q-2}}{a_1 = b_1} .
\end{array}$$

If a_p and b_q occur in S (or in E) then nothing need be done to this fragment; otherwise, a_p is b_q and this fragment should be replaced by

$$\begin{array}{c}
\frac{a_1 = a_1 \quad E_{p-1}}{a_1 = a_2} \\
\vdots \\
\frac{a_1 = a_{p-1} \quad E_1}{a_1 = a_p \quad E_p} \\
\frac{a_1 = b_{q-1}}{a_1 = b_{q-1}} \\
\vdots \\
\frac{a_1 = b_2 \quad E_{p+q-2}}{a_1 = b_1} .
\end{array}$$

Finally, obtain T_s by deleting inferences of the form

$$\frac{a = c \quad b = b}{a = c}$$

from the resulting computation. $\square$

3.5. PROPOSITION. *If T is a singular computation of E from S , then there is a singular computation T_w of E from S with the weak subterm property of length $\leq (\text{lh}(T))^2 + \text{lh}(T) + 1$.*

PROOF. Let $\text{lh}(T) = n$. We proceed inductively over larger and larger subcomputations of T which end in inferences of the form (2), replacing these by new computations (however, we will continue to refer to the computation at stage k as “ T ”). At each stage we consider the H fragment containing the premiss of one such inference; if the corresponding subcomputation of the original T has length p then this fragment has at most length $2p$. The fragment is converted into one of at most length $p + 2$ and then into a K computation of at most length $2p + 2$, which is substituted for it in the larger computation (while the inference of the form (2) is deleted).

At most $p + 2$ of the $2p + 2$ equations are "passed on" to the next H fragment, and one equation has been deleted altogether; the bound $n^2 + n + 1$ follows easily.

Stage 1: Replace each maximal subcomputation of the form

$$\frac{s^q a = s^q a}{s^{q-1} a = s^{q-1} a}$$

$$\vdots$$

$$\frac{sa = sa}{a = a}$$

by $a = a$.

Stage $k + 1$: Select a minimal subcomputation of T ending in an inference of the form (2) which has not yet been considered, and consider the H fragment containing $sa = sb$. If this fragment is just $sa = sb$, then do nothing (since we are at stage $k + 1$, the subcomputation ends in two successive inferences of the form (2) and sa and sb occur in S since ssa and ssb do). Otherwise, by the transformations of Proposition 3.4, obtain from this fragment an H computation of the form

$$\frac{sa = t_0 \quad E_0}{sa = t_1}$$

$$\vdots$$

$$\frac{sa = t_m \quad E_m}{sa = t_{m+1}},$$

where t_0 is sa , t_{m+1} is sb , t_i is not t_{i+1} , and by induction hypothesis each term occurring in the E_i occurs in S (if in the second step of the transformation of Proposition 3.4 a_p and b_q occur in S or E , then the inference

$$\frac{a_1 = a_p \quad a_p = b_q}{a_1 = b_q}$$

should be inserted at the appropriate place). We distinguish two cases:

- (i) each t_i has the form sr_i , and
- (ii) otherwise.

We treat case (ii) first, reducing it to case (i) for a smaller computation.

Case (ii). Select those pairs i, j such that

(a) t_{i-1} is sr_{i-1} ,

(b) t_i is not sr_i , and

(c) j is the smallest number larger than i such that t_j is again sr_j ;

then for each such pair E_{i-1} is $t_{i-1} \doteq t_i$, E_{j-1} is $t_{j-1} \doteq t_j$, and t_{i-1} and t_j occur in S . Replace each segment

$$\frac{sa = t_{i-1} \quad t_{i-1} \doteq t_i}{sa = t_i}$$

$$\vdots$$

$$\frac{sa = t_{j-1} \quad t_{j-1} \doteq t_j}{sa = t_j}$$

by

$$\frac{t_{i-1} = t_i \quad E_i}{t_{i-1} = t_{i+1}}$$

$$\vdots$$

$$\frac{t_{i-1} = t_{j-1} \quad E_{j-1}}{sa = t_{i-1} \quad t_{i-1} = t_j}$$

$$sa = t_j$$

and consider the fragment obtained by replacing each such replacement by its last inference

$$\frac{sat_{i-1} \quad t_{i-1} = t_j}{sa = t_j}$$

under case (i).

Case (i). Replace $sa = t_i$ by $a = r_i$ throughout the given H computation, simultaneously replacing each inference of the form

$$\frac{sa = t_i \quad t_i \doteq t_{i+1}}{sa = t_{i+1}}$$

by

$$\frac{a = r_i \quad \frac{sr_i \doteq sr_{i+1}}{r_i \doteq r_{i+1}}}{a = r_{i+1}} \quad \square$$

4. Conclusion

4.1. The fact that direct computations are formalizable in K has many consequences. Just to mention one, the rules of K are the most efficient possible (up to a constant factor when computations are coded as sequences of equations) of any finite set of “analytic” rules, both with respect to the length of computations and the length of terms. We leave most of the details to the reader; the principal fact needed is the following

4.1.1. PROPOSITION. *If M is a measure and E is derivable from S , then there are substitution instances $E_1, S_1; \dots; E_n, S_n$ of E and S , and singular*

computations T_i of E_i from S_i satisfying: for each substitution θ there is a non-projecting θ_i and a computation T_θ such that

- (i) $\theta E = \theta_i E_i$,
- (ii) $\theta S = \theta_i S_i$,
- (iii) T_i reduces to T_θ , and
- (iv) $\theta_i T_\theta$ is M -direct.

PROOF. Given E and S , by anticipating all possible “projections”, one can find substitution instances $E_1, S_1; \dots; E_n, S_n$ such that

- (a) if E is derivable from S then for each i so is E_i from S_i , and
- (b) for each θ there is an i and a non-projecting θ_i with (i) and (ii).

Suppose that E is derivable from S and choose T_i a singular computation of E_i from S_i with the subterm property. Given θ choose i and θ_i as above; let $M^*(a) =_{\text{df}} M(\theta_i a)$, and apply Proposition 3.3 to T_i with respect to M^* in order to obtain T_θ . $\square$

4.2. Our analysis of singular computations does not, as it stands, settle the relationship of arbitrary computations to direct ones. In particular, it does not answer the following

Question. Is there an infinite sequence of pairs E_i, S_i and a number n such that there is a computation of E_i from S_i of length $\leq n$, but any direct computation of E_i from S_i has length at least i ?

However, using our analysis, one could give a negative answer to this question if one could prove the following

Statement. There is a function f such that if T is a computation of E from S then there are E^*, S^*, θ^* , and T^* satisfying

- (i) θ^* is non-projecting,
- (ii) $\theta^* E^* = E$,
- (iii) $\theta^* S^* = S$,
- (iv) T^* is a singular computation of E^* from S^* , and
- (v) $\text{lh}(T^*) \leq f(\text{lh}(T))$.

4.3. Finally, other classes of computations formalizable in K have been studied in connection with efficiency. For example, in STATMAN [1974], Chapter 2, the length of computations from axioms satisfiable by partial functions is compared with the length of those from “equivalent” axioms only satisfiable by total ones.

References

KREISEL, G. and J.L. KRIVINE

- [1967] *Elements of Mathematical Logic* (North-Holland, Amsterdam, 2nd revised printing 1971).

KREISEL, G. and W. TAIT

- [1961] Finite definability of number theoretic functions and parametric completeness of equation calculi, *Z. Math. Logik Grundlagen Math.*, 7, 28–38.

LIFŠIC

- [1968] Specialization of the form of deduction in the predicate calculus with equality and function symbols, *Proceedings of the Steklov Institute of Mathematics*, Vol. 98.

STATMAN, R.

- [1974] Structural complexity of proofs, Dissertation, Stanford University, Stanford, CA.

Theories of Finite Type Related to Mathematical Practice

SOLOMON FEFERMAN

Contents

1. Introduction	914
2. Closure conditions on universes and finite-type structures .	918
3. Relations of the closure conditions to mathematical practice	924
4. Theories of finite type based on the closure conditions .	929
5. Some second-order comprehension and choice schemes .	937
6. Transfinite induction, recursion and iterated principles	941
7. Recursion-theoretic models of finite type	949
8. Second-order content of the theories studied: proof-theoretical methods .	957
9. Sources for further topics	968
References	969

1. Introduction

1.1. Aims and interests

This is a survey of work on formal theories related to substantial portions of mathematical practice. Most of current mathematics is based on non-constructive set-theoretical principles, but in fact strikingly little of what is implicit in those principles is actually used (except, of course, in set theory itself). For example, the bulk of mathematical analysis may be developed within *the finite type structure over the natural numbers* $\mathbf{N}$ and indeed within type level three. (The type level of $\mathbf{N}$ is 0, of $\mathbf{N}^{\mathbf{N}}$ and of the real numbers is 1, of the real functions is 2, and of operators on such is 3.) *Transfinite types* appear in set theory by *transfinite iteration* of the power set operation. But where such iteration is used at all in analysis, it is applied only to operations *within a given type*. Practice may be regarded as deficient in that it does not pursue the potential resources of transfinite types; this view is borne out by recent results concerning determinateness of Borel games (cf. MARTIN [1975]). Nevertheless, there is interest in a logical analysis of practice, for reasons which will be given in a moment; the restriction to *low types* certainly makes such a project more feasible.

Viewed logically, the main existential principles within any given type $\mathbf{S}$ are *comprehension axioms* or *choice axioms*. The former assert that for each property ϕ of elements of $\mathbf{S}$ there exists the set of all objects in $\mathbf{S}$ having the property ϕ . The class of properties considered may be described precisely within a formal language and, again quite strikingly, the defining properties which are actually used are of *very low logical complexity* (in several senses). This makes an informative logical analysis of practice even more feasible.

On the face of it such a study should have the same kind of interest as familiar mathematical investigations of *what kind of problems can be solved by given limited means* such as ruler-and-compass constructions, and solutions by mechanical computation. There is a difference from the present study in that the means specified in these familiar cases were already understood informally in a quite clear-cut way. There is a similarity in that the restriction to given means of construction or solution in a certain area may be gratuitous or an historical accident; the study of what can be obtained by such means is thus also an occasion to consider whether the restrictions are of a deeper or intrinsic significance.

This last is the position taken in different viewpoints as to the foundations of mathematics which call for restrictions on the methods employed

or completely alternative developments. We have in mind particularly the ideas originating with Hilbert, Brouwer, Poincaré, and the Borel–Lebesgue school.

As is well known, Hilbert wished only to restrict (to a bare minimum) the methods which would be used to *justify* mathematics by consistency proofs of appropriate formal systems. Though this program has turned out to be untenable, the *theory of formal systems and proofs* to which it gave rise has turned out to be one of the principal tools of the work described below (cf. also Chapter D.2).

It is not necessary to go into the ideas for *constructivity* introduced by Brouwer since that is covered fully in Chapter D.5. Certain of the formal theories studied there are very similar to those considered here. A principal difference is that we follow mathematical practice here in assuming *classical logic*. (Other significant differences will be noted below.) It happens that one means to approach our problems is to reduce the classical theories to (formally) *intuitionistic theories* and then exploit the explicit interpretability of the latter.

The viewpoints of the French mathematicians mentioned above were never developed systematically by them. In this respect the logical interest of the present work lies in giving precise explanations of the ideas involved and in comparing them with practice as first tests of their viability.

Poincaré laid emphasis on the primacy of our conception of the natural numbers and the *indefiniteness* of the concepts of *function* and *set* (and particularly of $\mathbb{N}^{\mathbb{N}}$ and $\mathbb{R}$). This led him to reject the use of so-called *impredicative* definitions, such as defining a subset of $\mathbb{N}$ (or a real number) by a property ϕ which involves quantification over a presumed totality of *all* subsets of $\mathbb{N}$ (or over *all* of $\mathbb{R}$). The logical analysis of *predicativity* has made considerable progress, and will play a role in various connections below.¹

The Borel–Lebesgue school was also dominated by the idea of dealing only with explicitly definable sets and functions. The difference lay in permitting definitions built up by *transfinite recursion* as well as (possibly) accepting $\mathbb{R}$ as *fixed*. This viewpoint has not yet been explained in a precise way, but much light has been thrown on it by developments in recursion theory as well as in terms of formal theories extending those described below.

Finally, logicians may find the work here to be of interest simply because

¹ The terminology “predicative” is not used in the same way by all authors. We apply it to that part of mathematics which is ultimately reducible to our conception of the natural numbers (cf. 6.4.5 and 9.3 below).

it is a meeting ground of everyday mathematics with ideas and methods from proof theory, model theory, and recursion theory leading to a number of results which are satisfying in their own right.

1.2. Plan of the chapter

Much of the literature in this subject deals with systems of second order, including a number which were selected for study only on syntactic grounds. The present exposition differs by concentrating on finite-type theories which directly reflect logical features of practice and in which everyday mathematics is readily developed. One of the main logical problems then is to give information about the *second-order content* of these theories.²

We begin in Section 2 with informal consideration of some *closure conditions* on universes of sets and functions. The elementary closure conditions lead to finite-type structures. Further closure conditions include *quantification functionals* for each domain which is regarded as fixed (or definite) and *recursion functionals* for $\mathbb{N}$. In Section 3 there is a (necessarily) brief indication of the relationship of these closure conditions to various parts of mathematics.

In Section 4 we proceed to formulate a number of finite-type theories based on these closure conditions. They are also recast in the logically more familiar form of CA (*comprehension axiom*) schemes and AC (*axiom of choice*) schemes. The second-order parts of these theories include systems which have been studied in the literature such as $\Delta_1^1 - \text{CA}$, $\Sigma_1^1 - \text{AC}$, $\Pi_1^1 - \text{CA}$, $\Delta_2^1 - \text{CA}$; these are described in Section 5. In continuation, Section 6 presents principles of transfinite induction and recursion expressed in second-order form. This permits us to explain iteration of certain principles, such as for *ramified analysis*.

Several *recursion-theoretic models* for finite-type theories are presented in Section 7. They are used to establish some *independence results* for mathematical statements relative to those parts of practice developed within the given theories. In particular, a number of examples are given using finite-type models whose second-order section consists exactly of the *hyperarithmetical* functions and sets.

More precise information about the second-order content of the theories studied is obtained by various proof-theoretical methods in Section 8.

² This approach has been developed by me in various lectures and courses over the years since 1970 (beginning with FEFERMAN [1971]). As will be seen below, it is a synthesis of ideas and results due to many people. The plan here is derived from that of FEFERMAN [1978].

These include Gentzen's method of *cut-elimination* and its adaptation to *normalization* of terms, reduction to formally intuitionistic theories, and Gödel's method of *functional interpretation*. Since these methods are discussed at greater length in Chapters D.2 and D.5, only special features of their employment for the problems here are discussed. Many of the results take the form that a given finite-type theory T^ω is a *conservative extension* of a second-order fragment T^2 . Among the side results described are characterizations of the *provable well-orderings* of various theories.

Section 9 concludes with a brief indication of the literature on further topics. It is not within the scope of this chapter to develop finite-type theories of ordinals needed to reflect the Borel–Lebesgue approach. For this reason and as a principal illustration we have concentrated throughout on the predicative/impredicative distinction as it manifests itself both in mathematics and in formal systems.

Sections 2 and 3 may be read without any background in logic and Section 4 with only moderate background. Sections 5–8 require more experience but not much special knowledge except for parts of the theory of recursive and hyperarithmetical functions (for which cf. ROGERS [1967]).

1.3. Historical note

Theories of finite type go back to the beginnings of modern foundational work with Russell's introduction (in 1908) of the (predicative) *ramified theory of types* over an unspecified set of individuals. This was elaborated in the *Principia Mathematica* where the so-called "axiom of reducibility" was added simply to get around difficulties of developing mathematics in the ramified system. As later realized by Ramsey, this made it equivalent to the (impredicative) *simple* or *unramified theory of types*.

Hilbert formulated several theories of functions of finite type over $\mathbb{N}$ during the 1920's. A third-order functional theory over $\mathbb{N}$ is presented in HILBERT and BERNAYS [1939] (Supplement IV). CHURCH [1940] gave a theory of functionals of all finite types over $\mathbb{N}$ in the symbolism of the *typed λ -calculus*. All of these systems accepted full impredicative comprehension schemes as axioms. Church's theory is equivalent in strength to Zermelo set theory.

The consideration of constructively acceptable axioms for objects of finite type and specifically the recursion operators R is due to GÖDEL [1958]. This, together with the treatment of KLEENE [1959c] of recursion in quantification functionals, form the principal theoretical antecedents of the present work.

2. Closure conditions on universes and finite-type structures

2.1. Elementary closure conditions on universes of sets and functions

2.1.1. By a *universe* is meant a pair $\mathcal{U} = (\text{Set}_{\mathcal{U}}, \text{Fn}_{\mathcal{U}})$ of collections called, respectively, the *sets of* $\mathcal{U}$ and the *functions of* $\mathcal{U}$. Elements of the sets of $\mathcal{U}$ may in certain cases themselves be sets or functions of $\mathcal{U}$, but can also be objects of other kinds such as numbers.

NOTATION. (i) A, B, C, X, Y, Z range over $\text{Set}_{\mathcal{U}}$ and f, g, h range over $\text{Fn}_{\mathcal{U}}$. We use a, b, c, x, y, z for elements of sets not otherwise distinguished. Certain capital letters are used for specific functions.

(ii) $f: A \rightarrow B$ is written when $\text{Dom}(f) = A$ and $\text{Rng}(f) \subseteq B$, and fa for $f(a)$ when $a \in A$. $\text{Gr}(f)$ denotes the graph of f considered as a subset of $A \times B$. For $X \subseteq A$, $f \upharpoonright X$ is the restriction of f to X and $C_A(X)$ is the characteristic function of X relative to A , i.e., $C_A(X): A \rightarrow \{0, 1\}$, $(C_A(X))a = 0 \Leftrightarrow a \notin X$.

(iii) $\mathcal{P}_{\mathcal{U}}(A) = \{X \in \text{Set}_{\mathcal{U}} \mid X \subseteq A\}$, $(A \rightarrow B)_{\mathcal{U}} = \{f \in \text{Fn}_{\mathcal{U}} \mid f: A \rightarrow B\}$. When there is no ambiguity, the subscript $\mathcal{U}$ will be dropped, and $(A \rightarrow B)_{\mathcal{U}}$ is then denoted by $(A \rightarrow B)$ or B^A .

2.1.2. $\mathcal{U}$ is said to be *Cartesian closed*³ if it satisfies the following conditions.

- (1) $\{0, 1\} \in \text{Set}_{\mathcal{U}}$,
- (2) $A, B \in \text{Set}_{\mathcal{U}} \Rightarrow A \times B, (A \rightarrow B)_{\mathcal{U}}$ and $\mathcal{P}_{\mathcal{U}}(A)$ belong to $\text{Set}_{\mathcal{U}}$,
- (3) $f \in \text{Fn}_{\mathcal{U}} \Leftrightarrow \text{Gr}(f) \in \text{Set}_{\mathcal{U}}$,
- (4) $A \in \text{Set}_{\mathcal{U}}$ and $X \subseteq A \Rightarrow (X \in \text{Set}_{\mathcal{U}} \Leftrightarrow C_A(X) \in \text{Fn}_{\mathcal{U}})$,
- (5) for each combination A, B, C of sets of $\mathcal{U}$ the functions K, S, P, P_1, P_2 , and D defined as follows are all in $\text{Fn}_{\mathcal{U}}$ (where $a \in A$, $b \in B$, $f \in (A \rightarrow (B \rightarrow C))$, $g \in (A \rightarrow B)$, and $i \in \{0, 1\}$):

- (i) $Kab = a$ (the constant functions),
- (ii) $Sfga = fa(ga)$ (substitution),
- (iii) $Pab = (a, b)$, $P^1(a, b) = a$, $P^2(a, b) = b$ (pairing and projections),

$$(iv) \quad Dabi = \begin{cases} a & \text{if } i = 0, \\ b & \text{if } i = 1 \end{cases} \quad (\text{definition by cases}).$$

All the universes $\mathcal{U}$ considered in the following are assumed to be Cartesian closed

³ The terminology comes from category theory; only a concrete form of the notion is used here.

NOTATION AND REMARKS. (i) $fa_1 \cdots a_n = (\cdots (fa_1) \cdots) a_n$, i.e., association is to the left. We write $(A_1, \dots, A_n \rightarrow B)$ for $(A_1 \rightarrow \cdots \rightarrow A_n \rightarrow B)$, i.e., for $A_1 \rightarrow (\cdots \rightarrow (A_n \rightarrow B) \cdots)$. To specify domains we may use subscripts, e.g., $K_{A,B} \in (A, B \rightarrow A)$, $P_{A,B} \in (A, B \rightarrow A \times B)$, etc.

(ii) K, S are the *basic combinators* which serve to generate all functions explicitly definable by repeated application. The λ -notation for abstraction may be explained in terms of these (and conversely). Thus $I = I_A = \lambda x \in A. x$ is defined by $I = SKK$, and $C = \lambda f \in (A \rightarrow B) \lambda g \in (B \rightarrow C) \lambda x \in A. f(gx)$ by $C = S(KS)K$, etc.; cf. Chapter D.7.

(iii) Conditions (3) and (4) express interchangeability or equivalence of sets and functions. This is accepted in set-theoretical mathematics but not in constructive mathematics where sets (or properties) are in general undecidable though all functions (constructions) are computable (cf. Chapter D.5).

(iv) The subsets of any given set are closed under finite Boolean operations, as is seen by the equivalence of sets and functions and definition by cases.

(v) Ordinarily closure under the operations $A \mapsto \mathcal{P}_{\mathcal{U}}(A)$ and $A, B \mapsto (A \rightarrow B)_{\mathcal{U}}$ would be considered highly non-elementary, but that is only the case in the presence of comprehension principles which permit quantification over *any* set. Without such we may think of $\mathcal{P}_{\mathcal{U}}(A)$ simply as a grouping together of all objects of the same kind or *type* in $\mathcal{U}$, namely the subsets of A in $\mathcal{U}$ (and similarly for $(A \rightarrow B)_{\mathcal{U}}$).

2.1.3. The *finite types of $\mathcal{U}$ over $A_0, \dots, A_n$* are the sets generated from $A_0, \dots, A_n$ by closing under the operations $A, B \mapsto A \times B$, $(A \rightarrow B)_{\mathcal{U}}$, $\mathcal{P}_{\mathcal{U}}(A)$.

Type symbols σ are used to denote members A_{σ} of $\mathcal{U}$ thus generated: given symbols $\gamma_0, \dots, \gamma_n$ for the *ground types*, they are built up by formal operations $\sigma, \tau \mapsto \sigma \times \tau$, $(\sigma \rightarrow \tau)$, $[\sigma]$. Then $A_{\gamma_i} = A_i$, $A_{\sigma \times \tau} = A_{\sigma} \times A_{\tau}$, $A_{(\sigma \rightarrow \tau)} = (A_{\sigma} \rightarrow A_{\tau})$, and $A_{[\sigma]} = \mathcal{P}(A_{\sigma})$.

$\mathcal{U}$ is said to be of *finite type over $A_0, \dots, A_n$* if each set X of $\mathcal{U}$ belongs to some $A_{[\sigma]}$, i.e., is a subset of some A_{σ} .

2.1.4. Reducing the number of basic concepts; finite type structures

The definition of Cartesian closed universe taken above was chosen as one most convenient and natural for mathematical applications. We can, however, make some simplifications for universes of finite type over given sets, in one of the following two ways.

(1) Take a ground type γ_0 with $0, 1 \in A_{\gamma_0}$. Restrict to the types built up from $\gamma_0, \dots, \gamma_n$ by the operation $\sigma, \tau \mapsto (\sigma \rightarrow \tau)$. Subsets of A_{σ} are treated

in terms of their characteristic functions in $A_{(\sigma \rightarrow \gamma_0)}$. To dispense with pairing and projection, operations of several variables are replaced by unary functions and repeated application (e.g., $(\sigma_1 \rightarrow (\sigma_2 \rightarrow \tau))$ takes the place of $(\sigma_1 \times \sigma_2 \rightarrow \tau)$). *Partial functions* from (a subset B of) A_σ to A_τ are treated as restrictions of total functions in $A_{(\sigma \rightarrow \tau)}$ (which may be assigned values arbitrarily for arguments not in B). This is the approach that we shall actually follow in the logical development of Section 4–8.

(2) Types are built up only by the operations $\sigma, \tau \rightarrow \sigma \times \tau$, $[\sigma]$. In this case functions from A_σ to A_τ (partial or total) are identified with their graphs in $A_{[\sigma \times \tau]}$.

NOTE. Neither of these simplifications is suitable for constructive mathematics. For example, if f is a partial computable operation from A_σ to A_τ we cannot in general extend f to a total computable operation on A_σ .

2.2. Closure under quantification; choice operators

For any $\mathcal{U}$ and set A in $\mathcal{U}$, define the function(al) $\exists^A : \mathcal{P}(A) \rightarrow \{0, 1\}$ by

$$\exists^A X = 0 \Leftrightarrow X \text{ is non-empty.} \quad (1)$$

Equivalently (when $0 \in B$), define $\exists^A : (A \rightarrow B) \rightarrow \{0, 1\}$ by

$$\begin{aligned} \exists^A f = 0 &\Leftrightarrow \exists a \in A (fa = 0), \\ \exists^A f = 1 &\Leftrightarrow \forall a \in A (fa \neq 0). \end{aligned} \quad (2)$$

We say that $\mathcal{U}$ is $\exists^A$ -closed if $\exists^A$ is a function of $\mathcal{U}$.

By a *choice* or *selection operator* C for $\exists^A$ we mean a functional from $\mathcal{P}(A)$ to A such that

$$X \subseteq A \text{ and } \exists^A X = 0 \Rightarrow CX \in X. \quad (3)$$

2.3. Universes over the natural numbers

2.3.1. A structure $\mathfrak{M}$ is said to belong to $\mathcal{U}$ if all of its domains, relations, and functions are in $\mathcal{U}$.

Suppose the structure $\mathfrak{N} = (\mathbb{N}, 0, ')$ belongs to $\mathcal{U}$. i, j, k, n, m, p range over $\mathbb{N}$. The *N-recursion operators* are the functions R (or $R_A^{(n)}$) defined by:

$$Raf0 = a, \quad Rafn' = fn(Rafn) \quad (1)$$

for each A , $a \in A$, $f \in (\mathbb{N}, A \rightarrow A)$ and $n \in \mathbb{N}$. These functionals were introduced in GÖDEL [1958]. They have an *impredicative* or *non-elementary* character, illustrated as follows for $A = [\mathbb{N}^{\mathbb{N}} \rightarrow \mathbb{N}]$; here we take 'g' in place of 'a' and let h range over $\mathbb{N}^{\mathbb{N}}$.

$$Rgf0h = gh, \quad Rgfn'h = fn(Rgfn)h. \quad (2)$$

Writing $Rgfn$ as $\lambda h_1(Rgfnh_1)$ we see that $Rgfn'h$ depends *prima facie* on $Rgfnh_1$ for all h_1 in $\mathbb{N}^n$. Elementary recursion operators $\hat{R}$ (or $\hat{R}_A^{(n)}$) may be defined as follows for any $A = (B_1, \dots, B_n \rightarrow \mathbb{N})$:

$$\hat{R}gf0b = gb, \quad \hat{R}gfn'b = fn(\hat{R}gfnb)b \quad (3)$$

where $b = b_1, \dots, b_n$, each $b_i \in B_i$ and $g \in A$.

NOTE. The operators $\hat{R}$ are essentially those introduced by KLEENE [1959c]. It was shown there that the functions in $(\mathbb{N} \rightarrow \mathbb{N})$ generated by 0, 1, and all $K, S, \hat{R}$ are exactly the primitive recursive functions. A general recursive function which is not primitive recursive can be obtained using the operators R instead; familiar examples of such are defined by double recursion on $\mathbb{N}$, which may be recast as a single recursion on $\mathbb{N}^n$.

2.3.2. We say that $\mathcal{U}$ is $\hat{\mathbb{N}}$ -closed if it contains the structure $\mathfrak{N}$ and all of the elementary recursion operators $\hat{R}$. $\mathcal{U}$ is said to be $\mathbb{N}$ -closed if instead it contains all the recursion operators R . The functions of finite type over $\mathbb{N}$ generated by 0, ', and all K, S, R form the *primitive recursion functionals* (in Gödel's sense). From now on, all universes considered are assumed to be at least $\hat{\mathbb{N}}$ -closed.

2.3.3. In order to reflect that *quantification over $\mathbb{N}$* is accepted as definite, we may demand that $\mathcal{U}$ be $\exists^{\mathbb{N}}$ -closed.⁴ The *unbounded minimum operator* μ is a choice operator for $\exists^{\mathbb{N}}$, taking as its definition:

$$\mu X = \begin{cases} \text{least } n \text{ belonging to } X & \text{if } \exists^{\mathbb{N}} X = 0, \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

Since the graph of μ is definable from $\exists^{\mathbb{N}}$ and $<$ (and the latter is defined by primitive recursion), μ is in $\mathcal{U}$ iff $\exists^{\mathbb{N}}$ is in $\mathcal{U}$.

2.4. Universes over the real numbers

If the set of real numbers $\mathbb{R}$ and a structure on it, say $\mathfrak{R} = (\mathbb{R}, =_{\mathbb{R}}, +, \cdot, 0, 1)$, are considered as basic, then one may deal with universes which contain $\mathfrak{R}$ and are $\exists^{\mathbb{R}}$ -closed. If instead $\mathbb{R}$ is defined in terms of $\mathbb{N}^{\mathbb{N}}$ (as is done below), one may assume $\mathcal{U}$ to be $\exists^{(\mathbb{N} \rightarrow \mathbb{N})}$ -closed. Note that $=_{\mathbb{N}^{\mathbb{N}}}$ is

⁴ $\exists^{\mathbb{N}}$ is often denoted by 2E in the literature on recursive functionals of finite type. For reference below, $\exists^{(\mathbb{N} \rightarrow \mathbb{N})}$ is then denoted by 3E .

definable using $\exists^{\aleph}$. (We did not need to include $=_{\aleph}$ in $\aleph$ because it is definable by recursion.)

2.5. Closure conditions for well-foundedness, ordinals, and inductive definitions

2.5.1. Well-founded relations

We write $a < b$ for $(a, b) \in B$ when $B \subseteq A^2 = A \times A$ and B is transitive. The test for a relation B in A to be *well-founded (relative to $\mathcal{U}$)* is given via a functional $\exists \downarrow^A$ from $\mathcal{P}(A^2)$ into $\{0, 1\}$:

$$\exists \downarrow^A B = \begin{cases} 0 & \text{if } \exists f \in (\mathbb{N} \rightarrow A) \forall n [fn' <_B fn], \\ 1 & \text{otherwise.} \end{cases} \quad (1)$$

We emphasize that this test is relative to $\mathcal{U}$, as $<_B$ need not be well-founded in the absolute sense if $\exists \downarrow^A B = 1$: $(\mathbb{N} \rightarrow A)_{\mathcal{U}}$ may be a proper subset of the set of all functions from $\mathbb{N}$ into A .⁵ If B is truly well-founded we can apply the *principle of transfinite induction* to any subset X of A (whether or not X is a $\mathcal{U}$ -set):

$$\forall x \in A [\forall y (y <_B x \Rightarrow y \in X) \Rightarrow x \in X] \Rightarrow \forall x \in A (x \in X). \quad (2)$$

2.5.2. When A is $\mathbb{N}$ (or any other well-ordered set), we can define a selection operator L for the quantifier $\exists \downarrow^{\aleph}$ above in the sense that

$$\exists f \in (\mathbb{N} \rightarrow \mathbb{N}) \forall n [fn' <_B fn] \quad \text{and} \quad g = LB \Rightarrow \forall n [gn' <_B gn]. \quad (1)$$

For example, g may be described as the *leftmost branch through B* and g may be defined by recursion in terms of $\exists \downarrow^{\aleph}$. Note that testing for well-foundedness of $B \subseteq \mathbb{N}^2$ is weaker than use of $\exists^{(\aleph \rightarrow \aleph)}$.

2.5.3. Ordinals

These may be dealt with as equivalence classes of well-ordering relations. However, for a more natural treatment of closure conditions corresponding to practice one would consider countable ordinals as a ground type Ω_1 and would assume associated recursion operators $R^{(\alpha)}$ of finite type over Ω_1 . Similarly, uncountable ordinals would be treated using further ground types Ω_2, Ω_3 , etc. Because of limitations of space, we shall not pursue this here.

⁵ For example, in Section 7 we shall consider finite-type structures $\mathcal{U}$ over $\mathbb{N}$ in which $(\mathbb{N} \rightarrow \mathbb{N})_{\mathcal{U}}$ consists of just the hyperarithmetic functions. In this case there are examples of recursive B for which $\exists \downarrow^{\aleph} B = 1$ according to (1) but $<_B$ is not well-founded (with regard to all functions).

2.5.4. Inductive definitions

Suppose given certain *closure conditions on a set* $X \subseteq A$, which may be put in the form

$$\forall a \in A [C(a, X) \Rightarrow a \in X] \quad (1)$$

where C is a relation between A and $\mathcal{P}(A)$ such that

$$C(a, X) \ \& \ X \subseteq Y \Rightarrow C(a, Y). \quad (2)$$

We speak of the set S *inductively generated* by these closure conditions as the smallest set X which satisfies (1). It is familiar that S is set-theoretically definable in one of two ways, “from above” as

$$a \in S \Leftrightarrow \forall X \subseteq A [\forall X (C(x, X) \Rightarrow x \in X) \Rightarrow a \in X] \quad (3)$$

or “from below” using ordinals α and approximations S_α :

$$S = S_{\alpha_0} \text{ where } S_{\alpha_0} = S_{\alpha_0+1}, \text{ and } a \in S_\alpha \Leftrightarrow C\left(a, \bigcup_{\beta < \alpha} S_\beta\right) \text{ for each } \alpha. \quad (4)$$

The approach (3) implicitly involves the condition on a universe $\mathcal{U}$ that it contains $\exists^{(\mathcal{P}A)}$ or $\exists^{(A \rightarrow \mathcal{N})}$, while approach (4) implicitly involves some sort of ordinal closure conditions as just indicated in 2.5.3. Inductive definitions of this kind will come up at several points in our work but again cannot be pursued in full. They are discussed in detail in Chapter C.7.

2.6. Comparison of universes

There is no simple inclusion relation between universes. Given two universes $\mathcal{U}_1$ and $\mathcal{U}_2$ over $\mathcal{N}$, we can compare $(\mathcal{N} \rightarrow \mathcal{N})_{\mathcal{U}_1}$ with $(\mathcal{N} \rightarrow \mathcal{N})_{\mathcal{U}_2}$, e.g., the former may be included in the latter. But once we ascend to higher types, e.g., to $((\mathcal{N} \rightarrow \mathcal{N}) \rightarrow \mathcal{N})_{\mathcal{U}_1}$, comparability in the ordinary sense is lost because the domains of the functions involved are different. However, there is a sense in which we can talk about *maximal* and *minimal* universes of a certain kind, and which we now wish to indicate.

Suppose ground-type symbols $\gamma_0, \dots, \gamma_n$ are given and sets $A_{\gamma_i} = A_i$ are specified. For simplicity we consider only symbols built up by $\sigma, \tau \mapsto (\sigma \rightarrow \tau)$. The *maximal finite type structure* $\mathcal{U}_{\max}$ over $A_0, \dots, A_n$ is determined by:

$$A_{(\sigma \rightarrow \tau)} = (\text{the totality of functions } f : A_\sigma \rightarrow A_\tau). \quad (1)$$

This definition is supposed to be construed in some absolute set-theoretical sense.

We speak about structures $\mathcal{U}_{\min}$ only with reference to certain closure

conditions. For example, the *minimal Cartesian-closed structure* over $A_0, \dots, A_n$ should be that whose functions are built up only by application from all $K_{A_\sigma}, S_{A_\sigma, A_\tau}$. To explain this more precisely we consider *terms* $s, t, \dots$ built up by application from constants $K_{\sigma, \tau}$ and $S_{\sigma, \tau, \rho}$ of respective types $(\sigma \rightarrow (\tau \rightarrow \sigma))$ and $(\sigma \rightarrow (\tau \rightarrow \rho)) \rightarrow [(\sigma \rightarrow \tau) \rightarrow (\sigma \rightarrow \rho)]$. These terms are then *identified* according to the rules:

$$Kst \equiv s, \quad Sstu \equiv su(tu). \quad (2)$$

The objects of the minimal structure are just equivalence classes of terms; application is trivially defined. Similarly, one may deal with the *minimal $\mathbf{N}$ -closed structure* by considering terms built up using $0, ', K_\sigma, S_{\sigma, \tau, \rho}, R_\sigma$ and by extending the definition of $\equiv$ to correspond to (1) of 2.3.1. An elaboration of this approach brings us to questions of *normalization of terms* which will be discussed in 8.2.

NOTE. Clearly, minimal structures $\mathcal{U}$ generated by countably many closure conditions over countable ground sets will be countable.

3. Relations of the closure conditions to mathematical practice

This section is of necessity very brief and sketchy. Only a detailed development would give precise meaning to the statements considered and then only step-by-step comparison with actual mathematics would constitute a verification of the assertions. However, the following should give a good idea of the kind of relationship that is claimed. For illustrative purposes the emphasis is on analysis.

3.1. Relativization of notions to universes

Let $\mathcal{U}$ be any $\hat{\mathbf{N}}$ -closed universe.

3.1.1. Set-theoretical notions are relativized to $\mathcal{U}$ simply by speaking about $\mathcal{U}$ -functions and $\mathcal{U}$ -sets instead of arbitrary functions and sets. This induces a relativization of all further mathematical concepts expressed in terms of $\mathfrak{N}$ and in terms of pairing functions, application, sets, and membership. In particular, infinite sequences $\langle a_n \rangle_n$ of objects are identified with functions whose domain is $\mathbf{N}$. The classical notions are a special case obtained by taking $\mathcal{U}$ to be the maximal finite type structure $\mathcal{U}_{\max}$ over given ground types. However, two notions which are equivalent in $\mathcal{U}_{\max}$

need not be equivalent in general $\mathcal{U}$. This sometimes requires a judicious choice among definitions of concepts for the smoothest development.

3.1.2. The notion of *real number* is relativized to $\mathcal{U}$ either by taking reals to be $\mathcal{U}$ -sets which are Dedekind sections of rationals or to be $\mathcal{U}$ -sequences of rationals which satisfy the Cauchy convergence criterion. In the latter case, reals are identified by an equivalence relation in the usual way. The two approaches are equivalent in $\exists^{\aleph}$ -closed $\mathcal{U}$: to each Cauchy sequence $\langle r_n \rangle_n$ corresponds the section $\{r \mid \exists m \forall n \geq m (r \leq r_n)\}$. The arithmetical operations are easily extended to the $\mathcal{U}$ -reals for either definition. Note that Cantor's diagonal argument shows the set of $\mathcal{U}$ -reals to be *uncountable* in $\mathcal{U}$, but of course it may be countable outside of $\mathcal{U}$.

3.1.3. The notion of *metric space* S in $\mathcal{U}$ is defined from the reals in $\mathcal{U}$ as usual. S is called *separable (relative to $\mathcal{U}$)* if it contains a dense subsequence $\langle d_n \rangle_n$ in $\mathcal{U}$. S is called *complete (relative to $\mathcal{U}$)* if every Cauchy sequence $\langle x_n \rangle_n$ of elements of S which lies in $\mathcal{U}$ converges in S . All of the spaces treated in the restricted developments are complete and separable. These include all spaces of interest in classical mathematics. *Basic open sets* in S are spheres $S(x; r) = \{y \mid d_S(y, x) < r\}$ specified by a center x and radius r . The following definition of *open set* X is most convenient, namely as one specified by a $\mathcal{U}$ -sequence $\langle (x_n, r_n) \rangle_n$ where $X = \bigcup_n S(x_n; r_n)$. Note that such a union is in $\mathcal{U}$ when $\mathcal{U}$ is $\exists^{\aleph}$ -closed. *Closed sets* for the space S are complements $S - X$ with X open. If X is closed and $\langle x_n \rangle_n$ is a convergent subsequence (in $\mathcal{U}$) of X , then $\lim_{n \rightarrow \infty} x_n \in X$. However, if X is in $\mathcal{U}$ and closed under limits in this sense, it need not be the complement of an open set in S . It is clear how to go on to define *continuous function* $f: S_1 \rightarrow S_2$ where f is in $\mathcal{U}$, and S_1, S_2 are metric spaces. Following this further we may relativize the notions of *normed vector space*, *linear functionals*, *linear operators*, etc. Most interesting functions spaces used to illustrate these require theories of integration, which in turn require further closure conditions to be considered in 3.2–3.4. Also further notions such as *compact set*, *Borel set*, *measurable set* must be delayed for the same reason.

3.2. Mathematics in $\exists^{\aleph}$ -closed universes

This coincides with the practice of predicative mathematics. We suppose throughout 3.2 that $\mathcal{U}$ is $\exists^{\aleph}$ -closed.

3.2.1. It turns out that all of analysis to 1900 and a substantial portion of twentieth-century analysis can be relativized in a straightforward way to

any such $\mathcal{U}$. The actual execution of this is due (in effect) to Weyl (1918) for the classical theory of real continuous and complex analytic functions, extended further by Kondô, Lorenzen and Kreisel into a theory of measurable sets and functions.⁶ As a final indication of the extent of analysis covered one may refer to BISHOP [1967] (p. 9), where it is stated that each constructive theorem ϕ found by him is a substitute for a standard classical theorem ψ which follows from ϕ plus the "limited principle of omniscience"; the latter is simply an informal statement of closure under $\exists^N$.

3.2.2. Sets vs. sequences

At first sight it appears that there is a serious obstacle to such an extensive development, since the $\mathcal{U}$ -reals are *not* in general closed under sup and inf of bounded sets of reals in $\mathcal{U}$. An example of such a universe $\mathcal{U}$ will be given in 7.3. One easily sees the difficulty if reals are treated as lower Dedekind sections in $\mathbb{Q}$. Then a set A of reals is a subset of $\mathcal{P}(\mathbb{Q})$, and its sup should be $Y = \bigcup A = \bigcup X [X \in A]$. But then $r \in Y \Leftrightarrow \exists X [X \in A \text{ and } r \in X]$; this definition requires quantification over $\mathcal{P}(\mathbb{Q})$ which is not generally available in $\mathcal{U}$, so that Y need not be a $\mathcal{U}$ -set (and hence need not determine a $\mathcal{U}$ -real). Similarly for the same purpose one must quantify over $\mathbb{Q}^N$ or $\mathbb{N}^N$ if reals are treated as Cauchy sequences.

3.2.3. Compactness, completeness and continuity

There is no problem in dealing with $\sup_n x_n$ and $\inf_n x_n$ for bounded sequences of reals in $\mathcal{U}$ since these are definable in terms of $\langle x_n \rangle_n$ by use of $\exists^N$. All the mathematics which generalizes to $\exists^N$ -closed universes goes through by dealing systematically with sequences rather than sets at crucial points. As an example, one proves the *sequential* compactness of any closed interval $[a, b]$ in $\mathbb{R}$ by the usual subdivision argument. Given $\langle x_n \rangle_n$ in $[a, b]$, we successively divide by halves so that at each stage, $[a_k, b_k]$ is the leftmost interval which contains x_n for infinitely many n . Note that this combines use of $\exists^N$ and $\hat{R}$. From this result of course follows the *completeness* of $\mathbb{R}$ in its relativized sense. The usual topological notion of *compactness* in terms of arbitrary open coverings is not used at all with the given restricted closure conditions.

The properties of *real continuous functions* follow readily because it is sufficient to deal with their values at rational arguments. Hence

⁶ Cf. GRZEGORCZYK [1955] for a more modern reworking of Weyl's analysis, as well as LORENZEN [1965]. For the theory of measurability see LORENZEN [1951] and KREISEL [1962].

$\sup\{fx \mid a \leq x \leq b\}$, $\inf\{fx \mid a \leq x \leq b\}$ can be proved to exist and to be taken on by f when continuous on $[a, b]$.

3.2.4. The following illustrates Bishop's assertion above. One constructive form of *Brouwer's Fixed Point Theorem* is that if f is a continuous map of the unit disk D into itself, then for each ε there exists x with $d(fx, x) < \varepsilon$. Hence there exists a sequence $\langle x_n \rangle_n$ in D such that for each n , $d(fx_n, x_n) < 1/n$. The classical conclusion $\exists x \in D (fx = x)$ is a consequence by sequential compactness. However, one can also follow familiar classical proofs more directly: one assumes $\forall x \in D (fx \neq x)$ and obtains a contradiction. (See Sections 11 and 12.4 in Chapter D.5.)

3.2.5. Integration and measure

Riemann integration is of course treated sequentially in the standard way. More general theories of integration are nowadays derived from theories of *measure*. However, even *Lebesgue (outer) measure* requires the full $\inf$ operation on sets for its definition: $\mu^*(A) = \inf\{\mu(G) \mid G \text{ open, } A \subseteq G\}$. It is not a problem to define $\mu(G)$ for $G = \bigcup_n (a_n, b_n)$; given G as a union of intervals one can find such a representation with (a_n, b_n) disjoint and then take $\mu(G) = \sum_{n=0}^{\infty} (b_n - a_n)$. While one cannot make use of outer measure, there is no difficulty in dealing with *measurable sets* A : classically, these have the property that for each $\varepsilon > 0$ there exist open G and closed F with $F \subseteq A \subseteq G$ and $\mu(G - F) < \varepsilon$. By a *measure approximation to A* let us mean a sequence $\langle (G_n, F_n) \rangle_n$ (in $\mathcal{U}$) where each G_n is open, F_n is closed, $F_n \subseteq A \subseteq G_n$, and $\mu(G_n - F_n) < 1/n$. Then we can take $\mu(A) = \inf_n \mu(G_n)$. Further, we have closure of the measurable sets under countable union, when sequences $\langle A_m \rangle_m$ of such are given together with measure approximations $\langle (G_{mn}, F_{mn}) \rangle_{n,m}$. Similarly we may deal with the theory of *measurable functions* in terms of approximations by step functions. Thus the function spaces L_p are available relativized to $\mathcal{U}$. From this one may proceed to the theory of *Banach spaces* and *Hilbert spaces* with the L_p as principal examples

3.2.6. RELATIVIZED KÖNIG'S LEMMA. *A finitely branching but infinite tree X in $\mathcal{U}$ contains an infinite branch in $\mathcal{U}$.*

This holds in any $\exists^{\mathbb{N}}$ -closed universe $\mathcal{U}$ and can be proven by the usual argument. Taking an example of an infinite recursive binary tree without recursive branches, it is seen that the $\mathbb{N}$ -closure is not sufficient for this result.

Sequential compactness of $\mathbb{R}$ can be viewed as a consequence of König's Lemma. It also implies *compactness in first-order predicate calculus*. To carry out first-order model theory, one needs the satisfaction relation for any structure. This is provided for any *countable* structure by combining $\exists^{\aleph}$ and definition of a sequence of predicates $\langle \text{Sat}_n \rangle_n$ by recursion R . Thus *countable model theory* relativizes to any $\exists^{\aleph}$ -closed universe.

Another noteworthy consequence of König's Lemma is *Ramsey's Theorem* (for a proof of the implication see Chapter B.3).

3.2.7. Relativization to $\hat{\aleph}$ -closed structures

Closer inspection of the arguments shows that the relativization of analysis described above need use throughout only the elementary recursion operators $\hat{R}$ together with the K , S and $\exists^{\aleph}$. This depends on working systematically only with sequences and with countable dense subsets of spaces. However, the possibility of this restriction is not always immediate. For example, in the *Cauchy-Lipschitz Theorem* on existence of local solutions of first-order differential equations we define a sequence f_n of real functions by successive approximation involving integration. This standard proof goes through without change if we use R but must be handled more carefully when using only $\hat{R}$. On the other hand, the full operators R are needed to define satisfaction in countable structures. This will follow from results of Section 8.

3.3. Well-foundedness closure conditions

The countable ordinals and associated definition by recursion and proof by induction enter if one wishes to speak of *Borel sets* or *Baire functions* or the sequence of *derivatives of a closed set*. One may also mention here their use in algebra, e.g., in the structure theory of countable *Abelian groups* and modules. To relativize these in a natural way, one would wish to consider certain closure conditions using ordinals as one ground type. Alternatively, one could deal with ordinals via well-ordering relations.

A form of the test $\exists \downarrow^{\aleph}$ for well-foundedness may be used to define the *analytic sets* in *descriptive set theory*. The *recursion-theoretic hierarchies* which provide analogues of the Borel, analytic and other classifications also make heavy use of generalized inductive definitions, well-orderings, and transfinite induction and recursion in their definition and development. For example, the statement that any two well-orderings are comparable is used to prove the *reduction* and *uniformization theorems* for Π_1^1 sets.

3.4. $\exists^{\mathbb{R}}$ -closed structures

It is already evident from 3.2 where quantification over $\mathbb{R}$ enters analysis in an essential way, namely in the general theory of *measure*. One may also add the definition and study of *projective sets* in descriptive set theory.

As shown by FRIEDMAN [1970b], even $\exists^{\mathbb{R}}$ -closure of $\mathcal{U}$ is insufficient to generalize *Borel determinacy* to such $\mathcal{U}$. MARTIN [1975] has shown that impredicative transfinite types are essential for his solution of this problem.

3.5. The Axiom of Choice

This is not a closure principle of the kind we have been discussing in the preceding sections and does not follow from them. The *uncountable axiom of choice* is used to obtain such mathematically significant results as the *Hahn–Banach Theorem*, *maximal ideals* in Banach spaces, etc. BISHOP [1967] has found constructive substitutes for certain of these. His work suggests that there may be versions provable using some of the above closure conditions and which serve for concrete applications. The *countable axiom of choice* is true in some natural $\mathbb{N}$ -closed and $\exists^{\mathbb{N}}$ -closed structures, as we shall see in Section 7. In addition, we shall discuss results in Section 8 for some formal systems of finite type which show eliminability of certain forms of countable AC.

4. Theories of finite type based on the closure conditions

4.1. Syntax

4.1.1. Types

To simplify the logical work, from now on we shall use the reductions indicated in 2.1.4(1). The *type symbols* sufficient for all our purposes are generated as follows:

(i) 0 is a type symbol.

(ii) If σ, τ are type symbols, then so also is $(\sigma \rightarrow \tau)$.

0 is the type symbol for $\mathbb{N}$; $(\sigma \rightarrow \tau)$ is sometimes also denoted $(\sigma)\tau$. The type symbol n is defined by induction with

$$n + 1 = (n \rightarrow 0). \quad (1)$$

Each language L to be considered has a specified set of types $\text{Typ}(L)$ containing 0 and closed under *subtypes*. The *level* of a type symbol is defined by

$$\text{lev}(0) = 0, \quad \text{lev}(\sigma \rightarrow \tau) = \max(\text{lev}(\sigma) + 1, \text{lev}(\tau)). \quad (2)$$

Thus $\text{lev}(n) = n$. We write $(\sigma_1, \dots, \sigma_n \rightarrow \tau)$ for $(\sigma_1 \rightarrow \dots \rightarrow \sigma_n \rightarrow \tau)$, where parentheses are associated to the right. Note every $\sigma \neq 0$ is of the form $(\sigma_1, \dots, \sigma_n \rightarrow 0)$.

4.1.2. Terms

Every L to be considered has infinitely many variables of each of its types. These are denoted by a, b, c, x, y, z . (The type superscript a^τ is used with variables only when necessary to avoid ambiguity.) We also use k, n, m, p as variables of type 0 and f, g, h as variables of any type $(\sigma \rightarrow \tau)$. L is specified by a certain set of constant symbols of various types as well as operators and predicates of level 1, i.e., having only arguments of type 0. Among these always are the constant 0 of type 0, the operator Sc on type 0 and the predicate $=$ between type 0 objects. The terms of various types are generated as follows:

- (i) Each variable and constant of L of type τ is a term of type τ .
- (ii) If t is of type $(\sigma \rightarrow \tau)$ and s is of type σ , then ts is of type τ .
- (iii) If F is an n -ary level 1 operator of L and t_i is of type 0 ($1 \leq i \leq n$), then $F(t_1, \dots, t_n)$ is of type 0.

We write t' for $Sc(t)$, t for $t_1, \dots, t_n$, and st for $st_1 \dots t_n$.

4.1.3. Formulas

The *atomic formulas* are all those of the form $P(t_1, \dots, t_n)$ where P is an n -ary level 1 predicate of L and t_i is of type 0 ($1 \leq i \leq n$). In particular, $s = t$ is always a formula for s, t of type 0. The *formulas* are generated by $\neg, \wedge, \vee, \rightarrow, \forall, \exists$, the quantifiers being applied to variables of any type in L . $\phi, \psi, \theta, \dots, \phi(a), \phi(a, b), \dots$ range over formulas. Any formula may contain free variables (*parameters*) other than those indicated. By $\text{lev}(\phi)$ we mean $\max(\text{lev}(t))$ such that t occurs in ϕ . If $\mathcal{F}$ is any set of formulas, $n\text{-sec}(\mathcal{F})$ denotes the set of ϕ in $\mathcal{F}$ with $\text{lev}(\phi) \leq n$; this is called the *n -section* of $\mathcal{F}$ or the *$(n+1)$ -st order part of $\mathcal{F}$* . For each τ , variables X, Y, Z are introduced by convention to range over $(\tau \rightarrow 0)$ (which in this case might be denoted $[\tau]$), and we write

$$a \in X \leftrightarrow Xa = 0. \quad (1)$$

4.1.4. Equality at higher types and extensionality

For any type τ , we *define* the predicate $=_\tau$ of equality between objects of type τ inductively by

$$f =_{(\sigma \rightarrow \tau)} g \leftrightarrow \forall a^\sigma [fa =_\tau ga]. \quad (1)$$

Thus for $\tau = (\sigma_1, \dots, \sigma_n \rightarrow 0)$, $f =_\tau g \leftrightarrow \forall a_1^{\sigma_1}, \dots, a_n^{\sigma_n} [fa = ga]$. In order for these relations to satisfy the laws of equality one would have to accept all formulas

$$(Ext) \quad a =_\sigma b \rightarrow fa =_\tau fb$$

where f is of type $\sigma \rightarrow \tau$. From (Ext) and the laws of equality for type 0 we can then prove $[a =_\sigma b \wedge \phi(a) \rightarrow \phi(b)]$, i.e., that definitionally equal objects are indiscernible.

An alternative to this treatment would be to take $=_\tau$ as a basic predicate for each type τ and the laws of equality in all types as basic axioms. Then *extensionality* is expressed by the scheme

$$\forall x [fx =_\tau gx] \rightarrow f =_{(\sigma \rightarrow \tau)} g. \quad (2)$$

The principle (Ext) above has the same effect in our approach using definable equality at higher types. It is perhaps more natural for the mathematical applications to take equality at all types as basic, though extensionality need not be assumed. Our approach has some technical advantages, but we must show that (Ext) is eliminable; this will be discussed in 4.4.2.

NOTE. The subscript will be dropped in higher type equality when there is no ambiguity.

4.1.5. Number-theoretical axioms

Each theory **T** to be considered will use *classical logic* (unless otherwise specified) and will contain the following *axioms for 0 and Sc*:

- (i) $x' \neq 0$,
- (ii) $x' = y' \rightarrow x = y$.

Let $L = L(\mathbf{T})$ be the language of **T**. By the *induction scheme for $\mathbb{N}$* in L we mean all formulas of the form

$$(Ind^{\mathbb{N}}) \quad \phi(0) \wedge \forall n [\phi(n) \rightarrow \phi(n')] \rightarrow \forall n \phi(n)$$

where ϕ belongs to L . Unless otherwise restricted, each **T** will contain the *full induction scheme* $(Ind^{\mathbb{N}})$ in this sense. The only other case to be considered, and which is used only when $1 \in \text{Typ}(L)$, is the following (*restricted*) *induction axiom for $\mathbb{N}$* :

$$(I^{\mathbb{N}}) \quad 0 \in X \wedge \forall n [n \in X \rightarrow n' \in X] \rightarrow \forall n (n \in X).$$

4.1.6. Relations between theories

We put $T_1 \subseteq T_2$ when $L(T_1) \subseteq L(T_2)$ and every theorem of T_1 is a theorem of T_2 . We put $T_1 \equiv T_2$ if $T_1 \subseteq T_2$ and $T_2 \subseteq T_1$ (so $L(T_1) = L(T_2)$).

$\mathcal{F}$ is used to range over sets of formulas in a language $L = L(\mathbf{T})$. Unless otherwise specified, each $\mathcal{F}$ is assumed to contain all *basic formulas* (atomic formulas and their negations) and to be closed under $\wedge$ and $\vee$ (at least up to equivalence). The simplest example of such $\mathcal{F}$ that we shall consider is QF, the set of all *quantifier-free* formulas in L .

T_2 is said to be a *conservative extension* of T_1 for $\mathcal{F}$ if $T_2 \supseteq T_1$ and whenever $\phi \in \mathcal{F}$ and $T_2 \vdash \phi$, then $T_1 \vdash \phi$. T_2 is said to be a *conservative extension* of T_1 if this holds for the set $\mathcal{F}$ of all formulas in $L(T_1)$.

4.1.7. Schemata

Let σ be some type in L and $P(a)$ a predicate of variables a of type σ , which is not a predicate symbol of L . We write $L[P]$ for the language extended by P , and $\psi_s[P]$ for some fixed sentence of $L[P]$. Given any formula $\phi(a)$ of L , we take $\psi_s[\phi/P]$ to be the result of substituting $\phi(t)$ for $P(t)$ at each occurrence of the form $P(t)$ in $\psi_s[P]$. ϕ may contain free variables other than a ; these are called *parameters* of the substitution. If there are no such variables, we say that $\psi_s[\phi/P]$ is *without parameters*.

More generally, given any list $\sigma = (\sigma_1, \dots, \sigma_n)$ of types in L and predicate $P(a)$ of variables $a = (a_1^{\sigma_1}, \dots, a_n^{\sigma_n})$ we may define $\psi_s[\phi/P]$ for ψ_s in $L[P]$ and $\phi(a)$ in L . By a *scheme* (S) in L we mean the set of all formulas (called the *instances of the scheme*) of the form $\psi_s[\phi/P]$ for ϕ in L , associated with some fixed $\psi_s[P]$. By $(S)^-$ we mean the scheme using only instances without parameters. On the other hand, by $(\mathcal{F} - S)$ we mean the set of all instances $\psi_s[\phi/P]$ for $\phi \in \mathcal{F}$.

Still more generally, schemes may be determined as instances of given $\psi_s[P_1, \dots, P_k]$. In practice we shall describe schemes in terms of their instances.

For illustration, the scheme of induction (Ind^N) in L is determined by the formula $P(0) \wedge \forall n (P(n) \rightarrow P(n')) \rightarrow \forall n P(n)$. Then $(\text{QF} - \text{Ind}^N)$ denotes the set of all instances $\phi(0) \wedge \forall n (\phi(n) \rightarrow \phi(n')) \rightarrow \forall n \phi(n)$ for ϕ quantifier-free.

When dealing with σ of length $n = 1$ we can equivalently describe schemes in terms of formulas $\psi_s(X)$ where X is of type $(\sigma \rightarrow 0)$; then $\psi_s[\phi/X]$ is the result of substituting $\phi(t)$ for $(t \in X)$ at all such occurrences. In this sense (Ind^N) consists of all instances of I^N .

4.2. Comprehension and choice schemata

4.2.1. By the *Axiom of Choice* scheme we mean all formulas of the form

$$(AC) \quad \forall a \exists b \phi(a, b) \rightarrow \exists f \forall a \phi(a, fa).$$

$(AC_{\sigma, \tau})$ denotes the restriction of this scheme to variables a^σ, b^τ . $(AC_\sigma -)$ denotes $\bigcup_\tau (AC_{\sigma, \tau})$.

4.2.2. The (*general*) *comprehension axiom scheme for sets* is given by:

$$(CA) \quad \exists X \forall a [a \in X \leftrightarrow \phi(a)].$$

When the matrix ϕ of (AC) satisfies the unicity condition

$$\phi(a, b) \wedge \phi(a, c) \rightarrow b = c, \quad (1)$$

we have a form of *comprehension axiom for functions*. In particular, for any $\mathcal{F}$ and $\psi(a), \theta(a)$ in $\mathcal{F}$ take

$$\phi(a, n) \leftrightarrow \psi(a) \wedge n = 0 \vee \theta(a) \wedge n = 1.$$

Then

$$\forall a [\psi(a) \leftrightarrow \neg \theta(a)] \rightarrow \forall a \exists ! n \phi(a, n)$$

and the following *special comprehension axiom scheme for sets* is a consequence of $(\mathcal{F} - AC)$:

$$(\Delta_{\mathcal{F}} - CA) \quad \forall a [\psi(a) \leftrightarrow \neg \theta(a)] \rightarrow \exists X \forall a [a \in X \leftrightarrow \psi(a)]$$

for each ψ, θ in $\mathcal{F}$.

The class $\mathcal{F} = \text{QF}$ of quantifier-free formulas provides the simplest cases of interest of the relativized schemes in the following. Note that if $\bar{\mathcal{F}}$ denotes the set of ϕ equivalent to $\neg \psi$ where $\psi \in \mathcal{F}$, then $(\mathcal{F} - CA)$ and $(\bar{\mathcal{F}} - CA)$ are equivalent. Some evident second-order cases to consider are obtained using the classes $\Pi_\infty^0, \Sigma_1^1, \Pi_1^1$, etc., to be described in 5.1.

4.3. Defining axioms for finite type constants

The axioms for K, S and $R^{(n)}$ are given in each appropriate combination of types as follows:

$$(K) \quad Kab = a$$

$$(S) \quad Sfga = fa(ga)$$

$$(R) \quad Rfa0 = a, \quad Rfan' = fn(Rfan).$$

Recall that equality at higher types is considered to be defined according to 4.1.4. As noted in 2.3.1, all primitive recursive functions of natural numbers

can be defined using (K), (S), and (R), but also a recursive function which is not primitive recursive can be obtained.

NOTE. The use of the λ -notation for functions is justified in any theory containing the axioms (K) and (S).

Another particular consequence of (K), (S), (R) is *definition by cases*:

$$Dabn = \begin{cases} a & \text{if } n = 0, \\ b & \text{if } n \neq 0. \end{cases} \quad (1)$$

On the other hand, one can prove the existence of these various functionals from suitable simple instances of (AC): namely, K , S , D from (QF-AC) and the R -functionals from ($\mathcal{F}$ -AC) where $\mathcal{F}$ consists of formulas in (finite type) existential form.

4.4. Number theory in finite types

4.4.1. The language considered here uses all finite types generated from type 0, and all constants K , S , and R besides 0 and Sc . By the *theory of numbers in finite type*, denoted Z^ω , we mean the system with the following axioms:

- Z^ω
- (i) the axioms for 0, ',
 - (ii) the full induction scheme for $\mathbb{N}$,
 - (iii) the axioms (K), (S),
 - (iv) the axioms (R).

We shall consider extensions of Z^ω by various axioms and axiom schemata, e.g., $Z^\omega + (\text{Ext})$, $Z^\omega + (\text{QF-AC})$. In 4.6 we shall also consider finite type subsystems of Z^ω with restricted induction and/or elementary recursion operators.

4.4.2. Elimination of extensionality

We shall illustrate this for $Z^\omega + (\text{Ext})$. The same argument, which is due to Gandy (cf. LUCKHARDT [1973]), works for many other theories. Define $E_\tau(a)$ and $a \equiv_\tau b$ (a, b variables of type τ) for all τ inductively as follows:

- (i) $E_0(n) \leftrightarrow (n = n), \quad (n \equiv_0 m) \leftrightarrow (n = m).$
- (ii) $E_{\sigma \rightarrow \tau}(f) \leftrightarrow \forall a (E_\sigma(a) \rightarrow E_\tau(fa)) \wedge \forall a, b [a \equiv_\sigma b \rightarrow fa \equiv_\tau fb],$
 $f \equiv_{(\sigma \rightarrow \tau)} g \leftrightarrow \forall a (E_\sigma(a) \rightarrow fa \equiv_\tau ga).$

We now translate formulas ϕ of the language L of Z^ω into new formulas $\phi^{(E)}$ of the same language, by replacing each quantifier $\forall a^\tau (\dots)$ in ϕ by $\forall a^\tau [E_\tau(a) \rightarrow \dots]$ and similarly for $\exists a^\tau (\dots)$. Note that $\forall f^1 E_1(f)$ holds and more generally $\forall f^\tau E_\tau(f)$ holds for any τ of level 1. Thus if ϕ is a formula with all bound variables of level ≤ 1 , $\phi^{(E)}$ is equivalent to ϕ .

THEOREM. *If $Z^\omega + (\text{Ext}) \vdash \phi$ where ϕ is closed, then $Z^\omega \vdash \phi(E)$. Hence $Z^\omega + (\text{Ext})$ is conservative over Z^ω with respect to second-order formulas.*

PROOF. It is easily shown in Z^ω that each constant K , S , and R of type τ satisfies E_τ . Thus the inner model provided by $\langle E_\tau \rangle_\tau$ includes all the constants; the axioms of Z^ω clearly relativize. To prove $\phi^{(E)}$, where ϕ is any closure of an instance of (Ext) (4.1.4), note that $E_\sigma(a) \wedge E_\sigma(b) \rightarrow [(a =_\sigma b)^{(E)} \leftrightarrow a \equiv_\sigma b]$. $\square$

4.4.3. Countable and dependent choice schemes over Z^ω

The *countable axiom of choice* scheme in type τ consists of the formulas

$$(AC_{0,\tau}) \quad \forall n \exists b \phi(n, b) \rightarrow \exists f \forall n \phi(n, fn).$$

Related to this is the scheme for *dependent choices*

$$(DC_\tau) \quad \forall a \exists b \phi(a, b) \rightarrow \forall a \exists f [f0 = a \wedge \forall n \phi(fn, fn')]$$

with a, b of type τ . A neat generalization of the two is:

$$(GDC_\tau) \quad \forall n \forall a \exists b \phi(n, a, b) \rightarrow \forall a \exists f [f0 = a \wedge \forall n \phi(n, fn, fn')].$$

LEMMA. $(\mathcal{F} - GDC_\tau)$ follows from $(\mathcal{F} - AC_{\tau,\tau})$ in Z^ω .

PROOF. $(\mathcal{F} - AC_{\tau,\tau})$ implies $\forall n \forall a \exists b \phi(n, a, b) \rightarrow \exists h \forall n \forall a \phi(n, a, hna)$. Use (R) to obtain f with $f0 = a$, $fn' = hn(fn)$. $\square$

4.5. Systems with various quantification operators

These systems are suggested by the closure conditions considered in Section 2.3.

4.5.1. The numerical quantification operator

The language of Z^ω is enlarged by one new constant symbol $\exists^N$ of type 2, with the axioms

- ($\exists^N$) (i) $\exists^N X = 0 \vee \exists^N X = 1$,
 (ii) $\exists^N X = 0 \leftrightarrow \exists n (n \in X)$,

where X is of type 1. The resulting system is denoted $Z^\omega + (\exists^N)$.

4.5.2. Type 1 quantification operators

To quantify *over* type 1, i.e., $(0 \rightarrow 0)$, which intuitively denotes $(\mathbb{N} \rightarrow \mathbb{N})$, we use a type 3 constant $\exists^{N \rightarrow N}$ with the axioms

- ($\exists^{N \rightarrow N}$) (i) $\exists^{N \rightarrow N} X = 0 \vee \exists^{N \rightarrow N} X = 1$,
 (ii) $\exists^{N \rightarrow N} X = 0 \leftrightarrow \exists f (f \in X)$

where X is of type 2 and f of type 1.

Corresponding to the test for descending sequences discussed in 2.5 we have an operator $\exists \downarrow^N$ which quantifies over type 1 but in a more special way. Namely, $\exists \downarrow^N$ is a constant of type 2 with the axioms

- ($\exists \downarrow^N$) (i) $\exists \downarrow^N X = 0 \vee \exists \downarrow^N X = 1$,
 (ii) $\exists \downarrow^N X = 0 \leftrightarrow \exists f \forall n \langle fn', fn \rangle \in X$,

where X is of type 1, and $\langle m, p \rangle$ is a primitive recursive pairing function.

The resulting systems are denoted $Z^\omega + (\exists^{N \rightarrow N})$ and $Z^\omega + (\exists \downarrow^N)$, respectively.

4.6. Systems with restricted induction and/or recursion

4.6.1. Restricted induction

For any theory T considered above or in the following, *restricted-T* denotes the same theory with the induction scheme (Ind^N) replaced by the *induction axiom* (I^N) of 4.1.5. When T contains full (CA) , then $T \equiv \text{restricted-T}$. In general, though, *restricted-T* is much weaker than T ; a number of examples illustrating this will appear at various points below.

4.6.2. Elementary recursion

The elementary recursion operators in the sense of 2.3 (introduced by Kleene) are given by constants $\hat{R}$ with the axioms

- ($\hat{R}$) (i) $\hat{R}fanb = ab$,
 (ii) $\hat{R}fan'b = fn(\hat{R}fanb)b$

in all appropriate combinations of types for which ab is of type 0. Thus $=$ is $=_0$ in $(\hat{R})$. (If the list $b = b_1^{r_1}, \dots, b_k^{r_k}$ is empty, then a must be of type 0; otherwise a is of type $(\sigma_1, \dots, \sigma_k \rightarrow 0)$.) We denote by $\hat{Z}^\omega$ the system Z^ω with the axioms (R) replaced by the $(\hat{R})$. As we have observed in 2.3, the

primitive recursive functions are exactly those defined by closed terms of level 1 in $\hat{\mathbf{Z}}^\omega$.

We can of course go on to consider the subsystem *restricted- $\hat{\mathbf{Z}}^\omega$* . When formalizing the part of mathematics which generalizes to all $\hat{\mathbf{N}}$ - and $\exists^{\mathbf{N}}$ -closed structures as indicated in 3.2.7, it may be seen that induction is applied only to arithmetical properties, i.e., in which all quantifiers range over $\mathbf{N}$. In other words, it is formalized in *restricted- $\hat{\mathbf{Z}}^\omega + (\exists^{\mathbf{N}})$* . Naturally, the verification of this requires detailed consideration of the mathematical arguments utilized.

NOTE. The proof that $(\mathcal{F} - \text{AC}_{\tau, \tau})$ implies $(\mathcal{F} - \text{DC}_\tau)$ in $\mathbf{Z}^\omega$, given in 4.4.3, works only for $\tau = 0$ in $\hat{\mathbf{Z}}^\omega$, and in that case $(\mathcal{F} - \text{Ind}^{\mathbf{N}})$ suffices for the argument.

5. Some second-order comprehension and choice schemes

5.1. Special classes of second-order formulas

Consider the language L with just the types 0, 1. Take all primitive recursive functions as level 1 operators of L (or any subset from which these can be defined arithmetically, e.g., $+$, $\cdot$). A formula is said to be *arithmetical* if it contains no bound variables of type 1, though it may contain free variables of that type. The class of all such is denoted Π_x^0 . The subclass of Π_1^0 -formulas consists of all those in the form $\forall n \psi$ where ψ is quantifier-free. Proceeding as usual in the classification of analytic predicates, ϕ is said to be in Π_1^1 -form if $\phi = \forall f \psi$ where ψ is arithmetical, and in Σ_1^1 -form if $\phi = \forall f \psi$ with ψ arithmetical. Similarly, the Π_2^1 -formulas (Σ_2^1 -formulas) are those of the form $\forall f \exists g \psi (\exists f \forall g \psi)$ with ψ arithmetical. We also use the designations Π_1^0 , Π_x^0 , Π_1^1 , Σ_1^1 , etc. for the corresponding classes of formulas.

By $(\Delta_1^1 - \text{CA})$ we mean $(\Delta_{\mathcal{F}} - \text{CA})$ for $\mathcal{F} = \Sigma_1^1$; similarly for $(\Delta_2^1 - \text{CA})$ and $\mathcal{F} = \Sigma_2^1$. On the other hand, the classes Δ_1^1 , Δ_2^1 , etc. make sense only relative to a given theory T : ϕ is in Δ_1^1 (relative to T) if there are $\psi \in \Sigma_1^1$, $\theta \in \Pi_1^1$ such that T proves $(\phi \leftrightarrow \psi) \wedge (\psi \leftrightarrow \theta)$.

5.2. Second-order subtheories of $\hat{\mathbf{Z}}^\omega$

These are formulated in the language using only types 0, 1 including constants for all primitive recursive functions; we have seen that this may be considered part of $\hat{\mathbf{Z}}^\omega$. By *second-order arithmetic* we mean the system

$\mathbf{Z}^2$ in this language with (i) the axioms for 0, 1, and for each primitive recursive function, and (ii) the full induction scheme for $\mathbf{N}$. Again *restricted- $\mathbf{Z}^2$* takes induction only in the restricted form. Every second-order system considered below includes $\mathbf{Z}^2$ or *restricted- $\mathbf{Z}^2$* . $\mathbf{Z}$ denotes the usual system of first-order number theory.

5.3. Second-order comprehension and choice schemes

Let $\langle \ , \ \rangle$ be a primitive recursive pairing operation from $\mathbf{N} \times \mathbf{N}$ onto $\mathbf{N}$; for any f, n let $(f)_n m = f\langle n, m \rangle$, i.e., $(f)_n = \lambda m \cdot f\langle n, m \rangle$. This allows us to formulate second-order forms of $\text{AC}_{0,1}$, DC_1 , and GDC_1 as follows:

$$(\text{AC}) \quad \forall n \exists g \phi(n, g) \rightarrow \exists f \forall n \phi(n, (f)_n),$$

$$(\text{DC}) \quad \forall g \exists h \phi(g, h) \rightarrow \forall g \exists f [(f)_0 = g \wedge \forall n \phi((f)_n, (f)_{n'})]$$

$$(\text{GDC}) \quad \forall n \forall g \exists h \phi(n, g, h) \rightarrow \forall g \exists f [(f)_0 = g \wedge \forall n \phi(n, (f)_n, (f)_{n'})].$$

(Note that we are dropping type subscripts in the designations of these schemes.)

Each system obtained from $\mathbf{Z}^2$ by adjoining a scheme (S) will be named simply by its additional scheme (S), e.g., $(\Sigma_1^1 - \text{DC})$ denotes $\mathbf{Z}^2 + (\Sigma_1^1 - \text{DC})$. Similarly, *restricted- $(\Sigma_1^1 - \text{DC})$* denotes *restricted- $\mathbf{Z}^2$* + $(\Sigma_1^1 - \text{DC})$.

5.4. Second-order subsystems of some finite-type theories

5.4.1. Arithmetical comprehension in $\hat{\mathbf{Z}}^\omega + (\exists^\mathbf{N})$

Note that this system expresses the condition of closure under $\exists^\mathbf{N}$ for finite type structures.

All arithmetical formulas are equivalent to formulas built up by $\vee$, $\neg$, $\exists n$. This build-up can be reflected by terms, with primitive recursive functions taking care of the atomic formulas and propositional connective and the constant $\exists^\mathbf{N}$ taking care of numerical quantifiers. In other words, we obtain:

LEMMA. *For each arithmetical ϕ there is a term t with the same free variables as ϕ such that $(\phi \leftrightarrow t = 0)$ is provable in *restricted- $\hat{\mathbf{Z}}^\omega + (\exists^\mathbf{N})$* .*

COROLLARY. (i) $\hat{\mathbf{Z}}^\omega + (\exists^\mathbf{N}) \supseteq (\Pi_\infty^0 - \text{CA})$.

(ii) *The same holds for the corresponding restricted systems.*

5.4.2. Adding choice

THEOREM. (i) $\hat{\mathbf{Z}}^\omega + (\exists^\mathbf{N}) + (\text{QF} - \text{AC}) \supseteq (\Pi_\infty^0 - \text{AC})$.

(ii) $\mathbf{Z}^\omega + (\exists^\mathbf{N}) + (\text{QF} - \text{AC}) \supseteq (\Pi_\infty^0 - \text{DC})$.

(iii) *The same results hold for the corresponding restricted theories.*

PROOF. (i) is immediate by the lemma of the preceding section. For (ii) we also use (the proof of) the lemma of 4.4.3. $\square$

5.4.3. Easy comparisons of these second-order systems

THEOREM. (i) $(\Pi_1^0 - \text{CA}) \equiv (\Pi_\infty^0 - \text{CA})$.

(ii) $(\Pi_1^0 - \text{AC}) \equiv (\Pi_\infty^0 - \text{AC}) \equiv (\Sigma_1^1 - \text{AC})$.

(iii) $(\Pi_1^0 - \text{DC}) \equiv (\Pi_\infty^0 - \text{DC}) \equiv (\Sigma_1^1 - \text{DC})$.

(iv) $(\Pi_\infty^0 - \text{CA}) \subseteq (\Delta_1^1 - \text{CA}) \subseteq (\Sigma_1^1 - \text{AC}) \subseteq (\Sigma_1^1 - \text{DC})$.

(v) *The same results hold for the corresponding restricted theories.*

PROOF. We mention only three points which are involved. First, each arithmetical formula ϕ is shown (by induction) to define a set in $(\Pi_1^0 - \text{CA})$; the build-up of ϕ is reflected by operations on sets $- X$, $X \cup Y$, $\exists^\mathbf{N} X$. Second, if $\psi = \exists h \phi(g, h)$ where ϕ is arithmetical, then $\exists g \psi$ is equivalent to $\exists g \phi((g)_0, (g)_1)$. Hence choice principles for Σ_1^1 -matrices reduce to those for Π_∞^0 - and thence Π_1^0 -matrices. $\square$

NOTE. (i) $(\Pi_\infty^0 - \text{CA})$ has a finite axiomatization over $\mathbf{Z}^2$. The idea for this is contained in the first part of the proof just indicated. It is similar to the finite axiomatization of the Bernays–Gödel theory of sets and classes (with type 0 corresponding to sets and type 1 to classes).

(ii) It is essential for the proof that the formulas involved may contain second-order parameters. There is occasionally reason to consider the various schemes without parameters, as will be seen in Section 7.

The following generalizes (iv) above:

THEOREM. If $\mathcal{F} \supseteq \Pi_\infty^0$, then $(\Delta_{\mathcal{F}} - \text{CA}) \subseteq (\mathcal{F} - \text{AC}) \subseteq (\mathcal{F} - \text{DC})$.

5.4.4. The effect of choice with $(\exists \downarrow^\mathbf{N})$

THEOREM. (i) $\mathbf{Z}^\omega + (\exists \downarrow^\mathbf{N}) + (\text{QF} - \text{AC})$ proves $(\Sigma_2^1 - \text{DC})$.

(ii) $(\Delta_2^1 - \text{CA}) \equiv (\Sigma_2^1 - \text{AC}) \equiv (\Sigma_2^1 - \text{DC})$.

PROOF. (i) First note that $(\Sigma_2^1 - DC) \equiv (\Pi_1^1 - DC)$. The latter reduces to $(QF - AC)$ in $Z^\omega + (\exists \downarrow^\mathbb{N})$ by arguments previously used.

(ii) $(\Sigma_2^1 - DC) \subseteq (\Delta_2^1 - CA)$ is by formalization of the Kondô-Addison Theorem, according to which any Π_1^1 relation between type 1 functions can be uniformized. Standard proofs (see, e.g., ROGERS [1967]) make use of abstract countable ordinals. However, these can be treated by well-orderings in $\mathbb{N}$ as soon as we have comparability of well-orderings. The proof will be completed in Section 6.

NOTE. Addison and Kleene observed that the Δ_2^1 -predicates of natural numbers are closed under $(\exists \downarrow^\mathbb{N})$; a formal version of their argument is immediate. Δ_2^1 seems to be the syntactically simplest class with this property.

5.5. A restricted system conservative over Z

5.5.1. The following shows the weakening which can take place when induction for $\mathbb{N}$ is restricted to the axiom $(I^\mathbb{N})$. The result will be strengthened in Section 8.7.

THEOREM. (i) *Restricted $(\Pi_\infty^0 - CA)$ is a conservative extension of Z .*

(ii) *Restricted $\hat{Z}^\omega + (\exists^\mathbb{N})$ is a conservative extension of restricted $(\Pi_\infty^0 - CA)$.*

PROOF.^{6a} For (i) show that any model $\mathfrak{M}$ of Z can be transformed into a model $\mathfrak{M}^2$ of restricted $(\Pi_\infty^0 - CA)$. Take as the functions of the new model $\mathfrak{M}^2$ all $f: M \rightarrow M$ definable in $\mathfrak{M}$ by an arithmetical formula ϕ using parameters in M . Then the induction axiom $0 \in X \wedge \forall x [x \in X \rightarrow x' \in X] \rightarrow \forall x [x \in X]$ reduces for each X to an instance of the elementary scheme of induction, assumed true in $\mathfrak{M}$.

For (ii) we proceed similarly, only now beginning with an $\mathfrak{M}^2$ and forming a model $\mathfrak{M}^\omega$ (not necessarily extensional) with domains M_τ . These are defined by induction on $\text{lev}(\tau)$. Given $\tau = (\sigma_1, \dots, \sigma_n \rightarrow 0)$ and arithmetical $\phi(a_1^{\sigma_1} \cdots a_n^{\sigma_n}, y)$ permitting parameters from M_0, M_1 , or of level $< \text{lev}(\tau)$, such that $\forall a_1 \in M_{\sigma_1} \cdots \forall a_n \in M_{\sigma_n} \exists! y \phi(a, y)$, define $f_\phi a = y$ iff $\phi(a, y)$; M_τ is taken to consist of all such f_ϕ . It may be shown that each constant $K, S, \hat{R}$ has an interpretation in $\mathfrak{M}^\omega$ and that no new functions of type 1 arise. $\square$

5.5.2. Restriction is indeed a weakening in these cases:

^{6a} Note added in proof: The proof of part (ii) is not adequate as it stands, though the result is correct by the (even stronger) second theorem of 8.7.

THEOREM. *The consistency of $\mathbf{Z}$ is provable in $(\Pi_\infty^0 - \text{CA})$*

PROOF. There is a formula $\psi(n, X)$ which expresses that X is the set Tr_n of true first-order sentences of logical complexity $\leq n$. Using full induction for $\mathbb{N}$ we prove $\forall n \exists X \psi(n, X)$. The step $\forall X \exists Y [\psi(n, X) \rightarrow \psi(n', Y)]$ is elementary by the way in which Tr_{n+1} is arithmetically defined from Tr_n . Then we may apply induction again to prove that everything provable from $\mathbf{Z}$ is true. $\square$

6. Transfinite induction, recursion and iterated principles

The notions here can be applied to relations between type τ objects for any τ . However, most of the work in our subject concerns type 0. For example a common program is to characterize the arithmetical part or the 1-section of a finite type theory in terms of schemes of induction and recursion with respect to particular recursive well-orderings of natural numbers.

6.1. Well-foundedness and induction

6.1.1. Well-foundedness of orderings

Every $X \subseteq \mathbb{N}$ may be considered as a binary relation consisting of the pairs $\langle k, m \rangle$ with $\langle k, m \rangle \in X$; we write $k <_X m$ for $\langle k, m \rangle \in X$. Conversely each binary relation $<$ determines the set X of all $\langle k, m \rangle$ with $k < m$. We shall be considering relations given by formulas ψ :

$$(k < m) = \psi(k, m), \quad (1)$$

where ψ may contain parameters. Then the *well-foundedness* of $<$ is expressed by the formula

$$\text{WF}(<) = \neg \exists f \forall n \psi(fn', fn). \quad (2)$$

In particular, in $\mathbf{Z}^\omega + (\exists \downarrow^\mathbb{N})$, $\text{WF}(<_X)$ is equivalent to $\exists \downarrow^\mathbb{N} X = 1$. Clearly $\text{WF}(<)$ implies that $<$ is irreflexive; we do not assume that $<$ is transitive or connected. Finally, $\text{WF}(<)$ is also written $\text{WF}_<$ when $(k < m)$ is given by a formula (1) without parameters.

6.1.2. Induction on orderings

As we know on general set-theoretical grounds well-foundedness implies principles of transfinite induction and recursion. The latter will be considered in 6.2.

For any $<$ the scheme $\text{TI}(<)$ of *transfinite induction with regard to* $<$ (in any given language) consists of all formulas of the form

$$\text{TI}(<, \phi) \quad \forall m [\forall k < m \phi(k) \rightarrow \phi(m)] \rightarrow \forall m \phi(m),$$

where $\forall k < m \phi(k)$ abbreviates $\forall k (k < m \rightarrow \phi(k))$. The hypothesis of $\text{TI}(<, \phi)$ is sometimes called *the progressiveness* of ϕ .

When $<$ is $<_x$ we also write $\text{TI}(X, \phi)$ for $\text{TI}(<, \phi)$. When $<$ is given by a formula without parameters we write $\text{TI}_<(\phi)$. $\text{TI}(<, Y)$ is the instance of the scheme using the formula $\phi(k) = (k \in Y)$; thus we may also write $\text{TI}(X, Y)$ or $\text{TI}_<(Y)$ in case $<$ is $<_x$ or is defined without parameters. Finally, as with all our schemes, we may indicate restriction to a class $\mathcal{F}$; $(\mathcal{F} - \text{TI}(<))$ consists of all $\text{TI}(<, \phi)$ with ϕ in $\mathcal{F}$.

6.1.3. Induction on trees

Take a primitive recursive representation $\langle k_0, \dots, k_{n-1} \rangle$ of finite sequences by numbers; s, t range over such finite sequence numbers. When $s = \langle k_0, \dots, k_{n-1} \rangle$ put $\text{lh}(s) = n$, $s_i = k_i$, and $s \upharpoonright m = \langle k_0, \dots, k_{m-1} \rangle$ for $m \leq n$. We write $t \subseteq s$ if $t = s \upharpoonright m$ for some $m \leq \text{lh}(s)$, and $t \subset s$ for $t \subseteq s \wedge t \neq s$. Finally, $s * \langle l \rangle = \langle k_0, \dots, k_{n-1}, l \rangle$.

We say that X is a *tree* and write $\text{Tree}(X)$ if $\forall s, t [s \in X \wedge t \subseteq s \rightarrow t \in X]$. With each tree is associated the relation $s <_x t$ defined by $s \in X \wedge t \subset s$. (This is not to be confused with $<_x$ defined as in 6.1.1; the cases are distinguished by the styles of variables which are used.) For f of type 1 let $\bar{f}(n) = \langle f0, \dots, f(n-1) \rangle$. Then under weak hypotheses $\text{Tree}(X)$ implies

$$\text{WF}(<_x) \leftrightarrow \neg \exists f \forall n [\bar{f}(n) \in X]. \quad (1)$$

Under these hypotheses $\text{TI}(<_x, \phi)$ translates into

$$\forall s [s \notin X \rightarrow \phi(s)] \wedge \forall s [\forall k \phi(s * \langle k \rangle) \rightarrow \phi(s)] \rightarrow \forall s \phi(s). \quad (2)$$

6.1.4. Bar induction (well-foundedness implies induction)

For any formula $<$ the scheme $\text{BI}(<)$ of *bar induction with regard to* $<$ consists of all instances

$$\text{BI}(<, \phi) \quad \text{WF}(<) \rightarrow \text{TI}(<, \phi).$$

The terminology was introduced by Brouwer for principles applied to trees. Using (1) and (2) of 6.1.3, the scheme translates into a statement of bar induction very close to that used in the intuitionistic literature (cf. Chapter D.7, Section 10).

As with TI we may use the notations: $\text{BI}(X, \phi)$, $\text{BI}(<, Y)$, $(\mathcal{F} - \text{BI}_<)$, etc.

6.1.5. Some provable cases of bar induction

THEOREM. (i) $(\Pi_\infty^0 - CA) \vdash [WF(X) \leftrightarrow \forall Y TI(X, Y)]$.

(ii) If $\mathcal{F} \supseteq \Pi_\infty^0$, then $(\mathcal{F} - CA) \vdash BI(<_x, \phi)$ for each ϕ in $\mathcal{F}$.

PROOF. (i) Suppose $WF(X)$, i.e., there are no descending sequences in $<_x$. Given Y such that $\forall m [\forall k < m (k \in Y) \rightarrow m \in Y]$, to show $\forall m (m \in Y)$ holds. If not, there exists $m_0 \notin Y$. Further with each $m \notin Y$ we can associate $h(m) < m$ having $h(m) \notin Y$. By $(\Pi_\infty^0 - CA)$ there exists f such that $f0 = m_0$ and $\forall n f(n') = h(fn)$, contradicting $WF(X)$. Conversely, given $\forall Y TI(X, Y)$ and arbitrary f , in order to show $\neg \forall n f(n') <_x f(n)$ use Y defined by:

$$m \in Y \leftrightarrow \neg \exists n_0 (fn_0 <_x m \wedge \forall n \geq n_0 f(n') <_x f(n)).$$

(ii) is an immediate consequence of (i). $\square$

Of course under $(\mathcal{F} - CA)$ we can also write (ii) with $BI(<, \phi)$ for any relation $<$ in $\mathcal{F}$.

Though $(\mathcal{F} - CA)$ is formally required to establish $(\mathcal{F} - BI_<)$, the latter principle is generally perceived as being more elementary or basic than the former (particularly for familiar $<$).

6.1.6. Relationship with Π_1^1 -comprehension

By recursion theory, every Π_1^1 predicate $\phi(m, g)$ of numbers and functions can be brought to a normal form $\forall f \exists n P(m, \bar{f}(n), \bar{g}(n))$ where P is primitive recursive⁷; this argument uses only $(\Pi_\infty^0 - CA)$. The normal form may be read as expressing well-foundedness of the tree of s for which $\forall k \leq lh(s) \neg P(m, s \upharpoonright k, \bar{g}(k))$. Hence we have the following:

LEMMA. $(\Pi_1^1 - CA) \subseteq \hat{Z}^\omega + (\exists \downarrow^\omega)$.

Our interest now is to compare the second-order systems $(\Pi_\infty^0 - CA) + (BI)$ and $(\Pi_1^1 - CA)$. This will be a comparison as to strength since, as will be seen, neither is contained in the other. By 6.1.5 we know only that $(\Pi_1^1 - BI)$ and $(\Sigma_1^1 - BI)$ are contained in $(\Pi_1^1 - CA)$. The following was observed by Kreisel⁸:

⁷ For all such recursion-theoretic results the reader is referred to ROGERS [1967].

⁸ This, and various of the results below credited to Kreisel without reference, were first presented in the 1963 "Reports of a seminar on the foundations of analysis at Stanford", which was circulated but not published. A number of these are mentioned in KREISEL [1968].

THEOREM. $(\Pi_1^1 - CA)$ proves the existence of an ω -model for $(\Pi_\infty^0 - CA) + (BI)_< (< \text{ primitive recursive})$.

PROOF. The idea is to formalize the recursion-theoretic ω -model defined as the (enumerated) collection M_2 of all functions arithmetic in the set $\mathcal{O}$ of constructive ordinal notations. By the Kleene basis theorem (leftmost branch selection) for P primitive recursive

$$(\exists f \in M_2) \forall n [\bar{f}(n) \in P] \leftrightarrow \exists f \forall n [\bar{f}(n) \in P].$$

The existence of M_2 is provable in $(\Pi_1^1 - CA)$, as well as the definition of satisfaction for second-order formulas in M_2 . Then for any second-order ϕ with parameters in M_2 , the set defined by ϕ relative to M_2 is proved to exist in $(\Pi_1^1 - CA)$, so $BI(P, \phi)$ holds by the result of the preceding section. $\square$

There is a recursion-theoretic ω -model M_2 of $(\Pi_\infty^0 - CA) + (BI)$ using the same idea, relativized and iterated. Namely, take M_2 to consist of all f recursive in some $\mathcal{O}_n$ where $\mathcal{O}_0 = \mathbb{N}$ and $\mathcal{O}_{n+1} = \mathcal{O}^n$. Though a statement which expresses that $\mathcal{O}_n$ exists (for all n) can be proved in $(\Pi_1^1 - CA)$ and hence M_2 can be *defined* there, the truth definition for M_2 is not definable there. This gives interest to the following result of FRIEDMAN [1969], to which we refer the reader for a proof.

THEOREM. $(\Pi_1^1 - CA)$ proves the existence of an ω -model for $(\Pi_\infty^0 - CA) + (BI)$; it is conservative for Π_2^1 sentences.

6.2. Transfinite recursion

For a tree $X \subseteq \mathbb{N}$, one form of definition by *transfinite recursion* on X is: $fs = gs$ for $s \notin X$, $fs = hs(\lambda n, f(s * \langle n \rangle))$ for $s \in X$, where g, h are given functions. However, h must be of type 2 in this definition. Because of this transfinite recursion is more naturally dealt with in a finite type theory. For simplicity we shall only formulate here some second-order forms of recursion. Given a tree X , define $(f \upharpoonright_x s)$ of type 1 by:

$$(f \upharpoonright_x s)t = \begin{cases} ft & \text{if } t \subset s \text{ and } s \in X, \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

For a relation $<_x$ define

$$(f \upharpoonright_{<_x n})m = \begin{cases} fm & \text{if } m <_x n, \\ 0 & \text{otherwise.} \end{cases} \quad (2)$$

We write $\text{TR}(X, \phi, f)$ for $\forall s \phi(s, f \upharpoonright_x s, fs)$ when $\text{Tree}_1(X)$ and $\text{TR}(<_x, \phi, f)$ for $\forall n \phi(n, f \upharpoonright_{<_x n}, fn)$ in connection with relations. This is appropriate notation when $\phi(n, g, m)$ determines a functional $m = hng$, i.e., when $\forall n, g \exists! m \phi(n, g, m)$.

THEOREM. In $(\Delta_1^1 - \text{CA})$, $\Sigma_1^1 - \text{TI}(X)$ implies $\forall n \forall g \exists! m \phi(n, g, m) \rightarrow \exists! f \text{TR}(X, \phi, f)$ when ϕ is Σ_1^1 .

PROOF. By inspection of the standard argument for deriving transfinite recursion from transfinite induction. $\square$

Let CWO be the sentence expressing that if $<_x$ and $<_y$ are any two *well-ordering* relations, then $<_x$ is isomorphic to an initial segment of $<_y$ or vice versa.

COROLLARY. $(\Delta_1^1 - \text{CA}) + (\Sigma_1^1 - \text{BI}) \vdash \text{CWO}$.

As we have noted in 3.3, CWO is much used in the recursion-theoretic treatment of ordinals and in particular in the theory of $\mathcal{O}$ and Π_1^1 and hyperarithmetic predicates. For application of the theorem on recursion to hierarchies cf. 6.4.

We can also now complete the proof of the theorem in 5.4.5. In $(\Delta_2^1 - \text{CA})$ we can derive $(\Delta_1^1 - \text{CA})$ and $(\Sigma_1^1 - \text{BI})$, hence CWO. This is all we need to make use of well-ordering relations in place of ordinals.

6.3. Provably recursive well-orderings

6.3.1. Ordinal functions and associated well-orderings

For various specific ordinals α we have natural primitive recursive well-orderings $<_\alpha$ of order type α . These are given by orderings between terms built up from symbols for given ordinal functions. The most familiar, using $+$, $\cdot$, $\exp$, and Cantor normal form represents the segment up to $\alpha = \varepsilon_0 = \lim_n \omega_n$ where $\omega_0 = 1$, $\omega_{n+1} = \omega^n$. This is extended using successive *critical functions* $\kappa^{(\nu)}$ defined by

$$(i) \quad \kappa^{(0)}(\alpha) = \omega^\alpha,$$

$$(ii) \quad \kappa^{(\nu)} \text{ enumerates } \{\alpha \mid \forall \mu < \nu \kappa^{(\mu)}(\alpha) = \alpha\} \text{ for } \nu > 0.$$

Thus $\varepsilon_0 = \kappa^{(1)}(0)$. Let Γ_0 be the least ordinal such that $\nu, \alpha < \Gamma_0$ implies

$\kappa^{(\nu)}(\alpha) < \Gamma_0$; it may alternatively be described as the least solution of $\kappa^{(\nu)}(0) = \nu$. A natural primitive recursive well-ordering $<_{\Gamma_0}$ is obtained by using terms for the functions $+$, $\cdot$, $\exp$ and $\lambda\nu, \alpha \cdot \kappa^{(\nu)}(\alpha)$ (cf. SCHÜTTE [1960], FEFERMAN [1968]). For the present purposes when considering $<_a$ it is sufficient to take $\alpha \leq \Gamma_0$, and $<_a$ is the ordering of the initial segment of length $|a| = \alpha$. We write $a \oplus b$ and ω^a for primitive recursive functions on $<_{\Gamma_0}$ which make $|a \oplus b| = |a| + |b|$ and $|\omega^a| = \omega^{|a|}$. $\text{TI}(a, \phi)$ is $\text{TI}(<_a, \phi)$ and $\text{TI}(a)$ is the scheme of all such in any given language. Finally, $\text{I}(a)$ is written for $\forall Y \text{TI}(<_a, Y)$; this is equivalent to $\text{WF}(<_a)$ in $(\Pi_\infty^0 - \text{CA})$ by 6.1.5. Throughout, when a is specified and $\alpha = |a|$ we also write α for a , e.g., $\text{TI}(\alpha)$.

6.3.2. Induction below ε_0

Gentzen proved that $\mathbf{Z} \vdash \text{TI}(\alpha)$ for each $\alpha < \varepsilon_0$ and that this is best possible by showing $\text{TI}(\varepsilon_0, \phi) \rightarrow \text{Con}(\mathbf{Z})$ for a certain (quantifier-free) ϕ . SCHÜTTE [1960] has given a simple proof of the first fact. With $\phi(n)$ in any language we may associate $\phi^*(n)$ which is built up by numerical quantification from ϕ as follows:

$$\phi^*(a) \leftrightarrow \forall b [\forall c < b \phi(c) \rightarrow \forall c < b + \omega^a \phi(c)]. \quad (1)$$

LEMMA. $\text{TI}(a, \phi^*) \rightarrow \text{TI}(\omega^a, \phi)$ is provable in any extension of $\mathbf{Z}$.

The proof uses that if ϕ satisfies the progressiveness hypothesis of TI , so does ϕ^* .

COROLLARY. If $\mathbf{T}$ is any extension of $\mathbf{Z}$ and $\alpha < \varepsilon_0$, then $\mathbf{T} \vdash \text{TI}(\alpha)$.

The reason mentioned above for the bound ε_0 on $\mathbf{Z}$ will be discussed further in 8.2; in fact, it is the bound for any provable arithmetical ordering.

6.3.3. Strengthening a theory does not necessarily increase its stock of provably recursive well-orderings; e.g., this is the case with $\mathbf{Z} + \text{Con}(\mathbf{Z})$. However, adding stronger comprehension principles usually has that effect. The following shows the matter to be delicate. First, in $(\Pi_\infty^0 - \text{CA})$ the previous lemma allows us to prove $\forall Y_1 \exists Y_2 [\text{TI}(a, Y_2) \rightarrow \text{TI}(\omega^a, Y_1)]$, hence $\text{I}(a) \rightarrow \text{I}(\omega^a)$. By induction we then obtain $\text{I}(a) \rightarrow \text{I}(\varepsilon(a))$ where $\varepsilon(a)$ represents the next ε -number beyond a . Hence we also have $\text{I}(\varepsilon_b) \rightarrow \text{I}(\varepsilon_{b+1})$ in this theory. Applying $\text{TI}(\alpha, \phi)$ to $\phi(b) = \text{I}(\varepsilon_b)$ for $\alpha < \varepsilon_0$ we conclude:

LEMMA. $(\Pi_\infty^0 - CA) \vdash I(\gamma)$ for each $\gamma < \varepsilon_0$.

Curiously, though, there is still an instance of the *scheme* $TI(\varepsilon_0)$ which is *not* provable in $(\Pi_\infty^0 - CA)$. This is a special case of a general theorem of Kreisel which applies to *any finite extension of Z^2* and which will be discussed in 8.2. Of course in the theory $(\Pi_\infty^0 - CA) + (BI)$ we have $TI(\alpha)$ as soon as we have derived $I(\alpha)$. But there are also certain intermediate theories with this “balanced” property.

6.4. Iterated comprehension principles; ramified analysis

6.4.1. Jump operator hierarchies and iterated $(\Pi_1^0 - CA)$

The recursion-theoretic *jump operator* embodies $\exists^N$ as a functional $F: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$. In general, given such a functional F , a well-ordering relation $<$ in $\mathbb{N}$ and arbitrary X_0 we define $X = \langle (X)_n \rangle$ (n in the field of $<$) which iterates F along $<$; this is given by transfinite recursion as follows:

$$(i) (X)_0 = X_0,$$

$$(ii) (X)_{a \oplus 1} = F(X)_a,$$

$$(iii) \text{ for limit } a: x \in (X)_a \Leftrightarrow (x)_0 \in (X)_{(x)_1} \text{ and } (x)_1 < a.$$

X is called a *hierarchy for F along $<$ starting with X_0* . In (i)–(iii) we assume 0 is the least element under $<$ and $a \oplus 1$ is the successor of a in $<$. Suppose now that $<$ and $\lambda a. (a \oplus 1)$ are recursive and that the set of limit elements is recursive. Given a formal definition of $F(X) = Y$, write $\text{Hier}_<^F(X, X_0)$ to express that X satisfies (i)–(iii). If the definition of F may be given in second-order form so may the formula $\text{Hier}_<^F(X, X_0)$. In particular, this formula is arithmetical when F is the jump operator J . By 6.2 we can establish in $(\Delta_1^1 - CA) + TI(<)$ the statement $\forall X_0 \exists X \text{Hier}_<^J(X, X_0)$. This may also be considered as expressing the iteration of $(\Pi_1^0 - CA)$ along $<$. We write $(\Pi_1^0 - CA)_a$ for this statement along $<_a$ (when given a natural well-ordering of order-type α), and $(\Pi_1^0 - CA)_{<_\alpha}$ for the set of all statements $(\Pi_1^0 - CA)_\beta$ with $\beta < \alpha$ (using initial segments of a fixed $<_\alpha$). Since $(\Delta_1^1 - CA) \vdash TI(\beta)$ for each $\beta < \varepsilon_0$ by 6.3.2, we conclude:

THEOREM. $(\Delta_1^1 - CA) \supseteq (\Pi_1^0 - CA)_{<_{\varepsilon_0}}$.

6.4.2. Hyperjump hierarchy and iterated $(\Pi_1^1 - CA)$

We now apply the same ideas to hierarchies for the *hyperjump operator* J_1 which embodies $\exists \downarrow^N$. Write $(\Pi_1^1 - CA)_a$ for $\forall X_0 \exists X \text{Hier}_{<_a}^{J_1}(X, X_0)$ and $(\Pi_1^1 - CA)_{<_\alpha}$ for the set of all statements $(\Pi_1^1 - CA)_\beta$ for $\beta < \alpha$. While we

cannot apply the second-order statement of transfinite recursion 6.2 directly to this situation, it may be directly adapted to prove the following.

THEOREM. $(\Delta_2^1 - \text{CA}) \supseteq (\Pi_1^1 - \text{CA})_{<\varepsilon_0}$.

It is shown in FRIEDMAN [1970a] that the theorems of this and the preceding section are best possible; there are also analogous results for iterated $(\Pi_n^1 - \text{CA})$ with $n > 1$. We shall discuss the results for $n = 0, 1$ in Section 8.

6.4.3. Ramified analytic and hyperarithmetical sets

The basic step of predicative definition consists in passing from a collection $\mathcal{P}$ of subsets of $\mathbb{N}$ to the collection $\mathcal{P}^*$ of all subsets definable in the ω -model $\mathcal{P}$ from parameters in $\mathcal{P}$. The iteration of this procedure through all set-theoretic ordinals gives:

- (i) $\mathcal{P}_0 = (\phi)^*$ = the arithmetical sets,
- (ii) $\mathcal{P}_{\alpha+1} = \mathcal{P}_\alpha^*$,
- (iii) $\mathcal{P}_\lambda = \bigcup_{\alpha < \lambda} \mathcal{P}_\alpha$ for limit λ .

This is a second-order form of Gödel's notion of constructibility called the *ramified analytic sets*. It is known that $\mathcal{P}_\Omega$ (where Ω is the least uncountable ordinal) is a model of full second-order (DC). We are here concerned only with $\mathcal{P}_\alpha$ for $\alpha \leq \omega_1$ (the least non-recursive ordinal). $\mathcal{P}_{\omega_1}$ consists exactly of the *hyperarithmetical sets* as shown by KLEENE [1959a],

$$\mathcal{P}_{\omega_1} = \text{HYP}. \quad (1)$$

Recall that HYP consists of the sets recursive in some H_a for $a \in \mathcal{O}$; further, $H_a = (X)_a$ where $\text{Hier}_\omega^\perp(X, N)$ and $<$ is the predecessor relation along a path in $\mathcal{O}$ which includes a ; Spector showed that H_a and H_b are Turing equivalent when $|a| = |b|$. Let $\mathcal{H}_\alpha$ consist of the sets recursive in some H_a for $|a| < \alpha$. In more detail, Kleene showed that

$$\mathcal{P}_\alpha = \mathcal{H}_{\omega(1+\alpha)} \quad \text{for } \alpha < \omega_1. \quad (2)$$

Thus the ramified hierarchy up to ω_1 gives another form of iterating $\exists^\mathbb{N}$, so to speak ω steps at a time. When $\omega\alpha = \alpha$ we have $\mathcal{P}_\alpha = \mathcal{H}_\alpha$.

6.4.4. Ramified analysis and type theory

Given any ordinal α we can form a system of ramified analysis RA_α which uses numerical variables and set variables $X^{(\beta)}, Y^{(\beta)}, Z^{(\beta)}, \dots$ of degree β for each $\beta < \alpha$. The intended interpretation is that the variables of degree β range over $\mathcal{P}_\beta$. The axioms are those of $\mathbf{Z}$ plus full induction on

$\mathbb{N}$ in the language of RA_α , together with the *ramified comprehension axioms*:

$$(\text{RCA})_\alpha \quad \exists X^{(\beta)} \forall n [n \in X^{(\beta)} \leftrightarrow \phi] \quad \text{for each } \beta < \alpha,$$

where ϕ has each free second-order variable of degree $\leq \beta$ and each bound second-order variable of degree $< \beta$. In addition to the preceding, when $\alpha > \omega$ we must have an *infinitary rule of generalization* for each limit $\lambda < \alpha$, of the form

$$(\text{G})_\lambda \quad \text{Infer } \forall X^{(\lambda)} \phi(X^{(\lambda)}) \text{ from } \forall X^{(\beta)} \phi(X^{(\beta)}) \quad \text{for each } \beta < \lambda.$$

When α is the type of a recursive well-ordering the rule (G) may be partially expressed in finite form. RA_1 is a form of $(\Pi_\infty^0 - \text{CA})$ or $(\Pi_1^0 - \text{CA})_{<\omega}$. In general, if $\omega\alpha = \alpha$, RA_α is a form of $(\Pi_1^0 - \text{CA})_{<\alpha}$. It is shown in SCHÜTTE [1960] that RA_α proves $\text{TI}(\kappa^{(\beta)}(0))$ for each $\beta < \alpha$ when $\omega^\alpha = \alpha$. This will be discussed further in 8.2. The idea for ramified second-order theories may be extended to finite and transfinite type theory and set theory; for some formal systems of this kind, cf. SCHÜTTE [1960] and TAIT [1968].

6.4.5. Ramified progressions and predicativity

The idea of predicativity taken here is: that part of mathematical thought which is implicit in our conception of the natural numbers. Predicative definitions may involve quantification over sets and functions only restricted to collections specified by previously recognized classes of predicative definitions. Formally this is incorporated in *ramified progressions of theories* $\langle \text{RA}_\alpha \rangle_\alpha$. However, the general notion of well-ordering or ordinal is itself *prima facie* impredicative, so there must be some restriction on α . Kreisel had proposed the characterization in terms of *autonomous progressions*, where only those ordinals α are taken for which one has proved the existence of a representing well-ordering $<_\alpha$ of type α in a system RA_β with $\beta < \alpha$. Schütte and Feferman independently established Γ_0 to be the least impredicative ordinal under this proposal. Cf. FEFERMAN [1977] for the most recent discussion of work on this, including equivalent unramified systems of analysis.

7. Recursion-theoretic models of finite type

7.1. Introduction

We are interested here in models of various of the theories considered in Section 4, principally to get straightforward *independence results*, but also

to get some *conservative extension results* by formalizing their construction. The structures $\mathfrak{M}$ we deal with are specified by

- (i) a collection of sets M_τ , considered as the range of the type τ variables (for each τ in the language) where in all cases $M_0 = N$,
- (ii) *application operations* $\text{App}_{\sigma, \tau} : M_\sigma \times M_{\sigma \rightarrow \tau} \rightarrow M_\tau$ for each σ, τ , and
- (iii) interpretations of the constants.

The entire structure is indicated by $\mathfrak{M} = \langle \langle M_\tau \rangle_{\tau, \dots} \rangle$. We write fa for $\text{App}(f, a)$.

There are two notions of recursion in finite type which may be directly adapted to form models of theories considered in Section 4. The first is HEO, the *hereditarily extensional (effective) operations* (due to Kreisel) and the second is generated by Kleene's schemata S1–S9. The first is generalized to operations over any *enumerative structure* in 7.2; the second is only briefly described in 7.3. In the applications to the second-order content of the theories studied, one must have good information about the 1-section M_1 of $\mathfrak{M}$. This is immediate from the set-up in 7.2 but takes more work in the case of S1–S9 and its relativizations. However, it is more natural to consider the latter when one takes some finite type closure conditions as the starting point for a model. In both cases the models considered in this chapter are intermediate between the minimal structures for given closure conditions and the maximal structures discussed in 2.6.

7.2. Hereditary operations over an enumerative system

7.2.1. A suitable abstract notion of *enumerative system* $\mathfrak{E}$ generalizing the situation of ordinary recursion theory is presented in FRIEDMAN [1971], modifying previous notions of Wagner and Strong. The data for such $\mathfrak{E}$ are

- (i) a set A with at least two elements (the *domain* of $\mathfrak{E}$),
- (ii) collections $\mathcal{F}_1$ and $\mathcal{F}_2$ of unary and binary partial functions, respectively, of arguments in A to A ,
- (iii) total pairing and projection functions $P \in \mathcal{F}_2$, $P_1, P_2 \in \mathcal{F}_1$, and
- (iv) an *enumerating function* $f \in \mathcal{F}_2$ for $\mathcal{F}_1$; i.e., $\mathcal{F}_1$ consists of all functions $\lambda x. f(a, x)$ for $a \in A$.

$\mathfrak{E}$ is further required to satisfy:

- (v) $\mathcal{F}_1, \mathcal{F}_2$ are closed under composition,
- (vi) $\mathcal{F}_1$ contains the identity function and each constant function, and
- (vii) $\mathcal{F}_2$ contains each function $\text{DC}_{a,b} = \lambda x, y (a \text{ if } x = y; b \text{ otherwise})$ for definition by cases.

We write $\{a\}(x)$ or ax for $f(a, x)$ when f is the enumerating function specified in (iv). $\mathfrak{E}$ is said to be a *system over* $\mathbb{N}$ if $A = \mathbb{N}$ and the functions

$\mathcal{S}_c$ and $\mathcal{P}_d = \lambda x.(x - 1)$ are in $\mathcal{F}_1$. Only such $\mathcal{E}$ are considered in the following. It is easily shown that there is an $\mathcal{S}_1^1$ -function and that the *recursion theorem* holds in $\mathcal{E}$. The members of $\mathcal{F}_1$ may be referred to as the $\mathcal{E}$ -partial recursive functions, and the total members as the $\mathcal{E}$ -recursive functions (of one argument).

7.2.2. Hereditarily recursive and extensional operations over $\mathcal{E}$

Suppose given an enumerative structure over $\mathbf{N}$. The *hereditarily recursive objects of type τ over $\mathcal{E}$* , $\text{HRO}_\tau(\mathcal{E})$ are defined as follows:

(i) $\text{HRO}_0 = \mathbf{N}$, and

(ii) $\text{HRO}_{\sigma \rightarrow \tau} = \{a \mid \forall x (x \in \text{HRO}_\sigma \Rightarrow \{a\}(x) \in \text{HRO}_\tau)\}$.

We write $\text{HRO}(\mathcal{E})$ for $(\langle \text{HRO}_\tau(\mathcal{E}) \rangle_{\tau, \dots})$. The *hereditarily extensional effective objects of type τ over $\mathcal{E}$* are defined by interpreting E_τ of 4.4.2 in $\text{HRO}(\mathcal{E})$. Spelling this out again, HEO_τ and $a \equiv_\tau b$ are defined by induction:

(i) $\text{HEO}_0 = \mathbf{N}$ and $a \equiv_0 b \Leftrightarrow a = b$,

(ii) $a \in \text{HEO}_{\sigma \rightarrow \tau} \Leftrightarrow \forall x [x \in \text{HEO}_\sigma \Rightarrow \{a\}(x) \in \text{HEO}_\tau]$ and

$\forall x, y [x =_\sigma y \Rightarrow \{a\}(x) \equiv_\tau \{a\}(y)]$

$a \equiv_{(\sigma \rightarrow \tau)} b \Leftrightarrow \forall x [x \in \text{HEO}_\sigma \Rightarrow \{a\}(x) \equiv_\tau \{b\}(x)]$.

The structure $(\langle \text{HEO}_\tau(\mathcal{E}) \rangle_{\tau, \dots})$ is denoted $\text{HEO}(\mathcal{E})$. One easily interprets the K , S functionals in HRO and (using the recursion theorem) the recursion operators R of all types. These may be verified to be extensional, so one has:

THEOREM. *If $\mathcal{E}$ is any enumerative system, then $\text{HRO}(\mathcal{E})$ is a model of $\mathbf{Z}^\omega$ and $\text{HEO}(\mathcal{E})$ is a model of $\mathbf{Z}^\omega + (\text{Ext})$.*

7.3. Special cases

7.3.1. $\mathcal{E}$ given by ordinary recursion theory

Let $\mathcal{E}_1$ be the enumerative system of ordinary recursion theory. In this case it is known that HEO satisfies $(\text{QF} - \text{AC})$. This is remarked in KREISEL [1959a]; extending the result of Kreisel, Lacombe, Shoenfield for type 2 effective operations, one shows that every member of HEO is a *hereditarily continuous* (or *countable*) *functional*. The axiom of choice holds for the latter as proved by KLEENE [1959b]. The definition of $\text{HEO}(\mathcal{E}_1)$ can be formalized in arithmetic, as well as the proof that it satisfies $(\text{AF} - \text{AC})$. Hence we obtain the following improvement of the theorem in 4.4.2.

THEOREM. $\mathbf{Z}^\omega + (\text{Ext}) + (\text{QF} - \text{AC})$ is a conservative extension of $\mathbf{Z}$.

7.3.2. Π_1^1 recursion theory

One way to get a model for $(\exists^N)$ is to take $\mathfrak{E}_2$ to be an enumerative system for the partial Π_1^1 functions (obtained by uniformizing Π_1^1 relations). The $\mathfrak{E}_2$ -recursive functions are thus just the hyperarithmetic functions and the elements of $\text{HRO}(\mathfrak{E}_2)$ might be called the *hereditarily hyperarithmetic operations*. HARRISON [1968] showed that HYP is a model of Σ_1^1 -DC (extending KREISEL [1962]). It is reasonable to conjecture that $\text{HEO}(\mathfrak{E}_2)$ satisfies full (QF-AC). We have, at any rate:

THEOREM. *$\text{HEO}(\mathfrak{E}_2)$ is a model of $\mathbf{Z}^\omega + (\text{Ext}) + (\exists^N)$, in which the 1-section is HYP and hence a model of Σ_1^1 -DC.*

Note that formalizing the argument in this case does not lead to an obvious conservation result, since we need (BI) as well as $(\Delta_1^1 - \text{CA})$ to treat the properties of HYP. In this respect the proof-theoretical methods of Section 8 will be superior.

7.4. Recursive functionals of finite type

In KLEENE [1959c] partial recursive functionals are defined over the maximal type structure. Fixing one argument to be a given functional F , one gets a notion of being *partial recursive in F* . For any finite type τ over 0, this leads to $\text{Sec}_\tau(F) = \text{the set of objects of type } \tau \text{ which are (total) recursive in } F$. The structure $\mathfrak{M} = \text{Rec}(F) = (\langle \text{Sec}_\tau(F) \rangle_{\tau, \dots})$ satisfies $\mathbf{Z}^\omega$. By choosing F to correspond to given closure conditions, we may use $\mathfrak{M}$ to give models of theories embodying these closure conditions. For example, this holds with $F = \exists^N$ and $F = \exists \downarrow^N$. The following indicates some known relevant information about $\text{Rec}(F)$; cf. also Chapter C.6.

KLEENE [1959c] showed that $\text{Sec}_1(\exists^N) = \text{HYP}$. We know by Kleene's basis theorem that $\text{Rec}(\exists \downarrow^N)$ is a model of (BI). By Gandy's Selection Theorem (GANDY [1967]), $\text{Rec}(F)$ is a model of $(\Sigma_1^1 - \text{DC})$ for any F of type 2 in which $\exists^N$ is recursive. For such F , SHOENFIELD [1968] has given a hierarchy $\langle H_a^F \rangle_{a \in \mathcal{O}^F}$ for $\text{Sec}_1(F)$ which generalizes the hyperarithmetic hierarchy; this has length $\omega_1^F = \text{the least ordinal not (definable by a well-ordering) recursive in } F$. We denote by $\mathcal{H}_\alpha^F$ the set of functions recursive in some H_a^F of Shoenfield's hierarchy with $|a| < \alpha$. Thus $\mathcal{H}_\alpha^F$ coincides with the hyperarithmetical hierarchy for the ordinary jump operator J and $\mathcal{H}_\alpha^J$ is the *hyperjump hierarchy up to α* .

7.5. Independence results using REC

Take REC to be the set of recursive functions from $\mathbb{N}$ to $\mathbb{N}$. Studies in recursive mathematics have led to many counterexamples to statements of recursive analogues of classical theorems. These give independence results for such theorems from any finite type theory $\mathbf{T}$ which has a model $\mathfrak{M} = (\langle M_\tau \rangle_{\tau \dots})$ with $M_1 = \text{REC}$. In particular, $\mathbf{T} = \mathbf{Z}^\omega + (\text{Ext}) + (\text{QF} - \text{AC})$ is such a theory by 7.3.1.

For examples of such statements one may refer to 5.8, 5.9, 5.14 and 8.2 in Chapter D.5. In addition to those mentioned there, we may note two results of $\hat{\mathbf{Z}}^\omega + (\exists^\mathbb{N})$ which were discussed in Section 3 above, namely König's Lemma (KL) and Ramsey's Theorem (RT). It is familiar that KL is false in REC, using an infinite recursive binary tree with no branches (of length ω) in REC. Since KL implies RT, this is improved by the result of SPECKER [1971] showing Ramsey's Theorem also to be false in REC.

7.6. Independence results using HYP

There is also much detailed information about HYP which is useful in obtaining independence results from any theory which has a model $\mathfrak{M} = (\langle M_\tau \rangle_{\tau \dots})$ with $M_1 = \text{HYP}$. As we have seen, $\mathbf{Z}^\omega + (\text{Ext}) + (\exists^\mathbb{N}) + (\Sigma_1^1 - \text{DC})$ is such a theory.

7.6.1. Some facts about HYP

KLEENE [1959a] showed that every predicate $\psi(n)$ which is in Σ_1^1 -form relativized to HYP, i.e., of the form $\psi(n) \leftrightarrow \exists f_{\text{HYP}} \phi(n, f)$ with ϕ arithmetical, is in Π_1^1 . Spector proved the converse. We state the pair of results as

$$(\Sigma_1^1)^{(\text{HYP})} = \Pi_1^1. \quad (1)$$

Of course then $(\Pi_1^1)^{(\text{HYP})} = \Sigma_1^1$. GANDY [1960] gave a new proof of Spector's result; the main step was to show: if $<_\rho$ is a recursive linear ordering which is well-founded with respect to all HYP descending sequences but not well-founded, then the longest initial well-ordered segment of $<_\rho$ is of order type ω_1 . Hence there exist Π_1^1 well-orderings of order type ω_1 . This was proved independently in FEFERMAN and SPECTOR [1962], where an extension $\mathcal{O}^*$ of $\mathcal{O}$ was defined, partially ordered by a recursively enumerable $<$ behaving locally like $<_\rho$; $b \in \mathcal{O}^*$ holds by definition iff the set of $<$ -predecessors of b is well-founded with respect to HYP. By (1), $\mathcal{O}^* \in \Sigma_1^1$, so $\mathcal{O}^* - \mathcal{O}$ is nonempty. Taking any $a \in \mathcal{O}^* - \mathcal{O}$, it was shown that $\{x \mid x < a\}$ is a Π_1^1 -path through $\mathcal{O}$. Further, $\mathcal{O}$ and $\mathbb{N} - \mathcal{O}^*$ give an example of sets inseparable by any set in HYP; *a fortiori*, $\mathcal{O}^* \notin \text{HYP}$.

7.6.2. $(\Pi_1^1 - \text{CA})$ and (BI) are false in HYP.

Since the Π_1^1 definition of $\mathcal{O}$ relativized to HYP gives exactly $\mathcal{O}^*$, the following is an immediate conclusion.

THEOREM. $(\Pi_1^1 - \text{CA})$ without parameters is false in HYP.

The next was proved by Kreisel.

THEOREM. $(\Sigma_1^1 - \text{BI}_{<})$ is false in HYP for a primitive recursive $<$.

PROOF. Choose a linear primitive recursive $<_P$ which is well-founded with regard to HYP but not well-founded. Consider the predicate $\psi(n) \leftrightarrow \forall f [f0 <_P n \rightarrow \exists m (fm' \not<_P fm)]$ which expresses that $\{m \mid m <_P n\}$ is well-founded. By Spector's theorem $\psi(n)$ is equivalent to $\exists g_{\text{HYP}} \phi(n, g)$ with ϕ arithmetical. Let $\psi_1(n)$ be $\exists g \phi(n, g)$, so $\psi(n) \leftrightarrow (\psi_1(n))^{\text{HYP}}$. Since $\forall n [\forall m <_P n \psi(m) \rightarrow \psi(n)]$ is true we have $\forall n [\forall m <_P n \psi_1(m) \rightarrow \psi_1(n)]$ true in HYP. But $\text{HYP} \models \forall n \psi_1(n)$ would imply $\forall n \psi(n)$; a contradiction. $\square$

7.6.3. Some mathematical statements which are false in HYP

THEOREM. The l.u.b. principle is false in HYP.

PROOF. Take an arithmetical ϕ s.t. $\exists f_{\text{HYP}} \phi(n, f)$ is (in Π_1^1 but) not in HYP. Using the representation of reals, by Dedekind sections it may be shown that $\bigcup X[\phi(X), X \text{ Dedekind}, X \in \text{HYP}]$ is also not in HYP. $\square$

THEOREM. CWO is false in HYP.

PROOF (Kreisel). The idea is to use two HYP inseparable predicates $\forall f \exists x P_1(\bar{f}(x), n)$, $\forall f \exists x P_2(\bar{f}(x), n)$; the union of their complements A_1 , A_2 is $\mathbb{N}$. A_1 , A_2 may be written in the form $\forall f_{\text{HYP}} \exists x Q_1(\bar{f}(x), n)$, $\forall f_{\text{HYP}} \exists x Q_2(\bar{f}(x), n)$ respectively, with Q_1 , Q_2 recursive. Now if comparability of well-orderings held in HYP we could form a reduction of these complements, i.e., $A_1 \cup A_2 = A'_1 \cup A'_2$ where A'_1 , A'_2 are disjoint and in Π_1^1 form relative to HYP. But then $A'_1, A'_2 \in \Sigma_1^1$, so $A'_1 \in \text{HYP}$, contradicting the hypothesis. $\square$

7.6.4. By the representation (3.1) of open sets in $\mathbb{R}$ as unions of sequences of rational intervals, and of closed sets as complements of open sets, one

can formulate various statements concerning these in second-order terms and test them in HYP. The theorem of Cantor–Bendixson (C–B) states that every closed set F has a *perfect kernel* $F^* \subseteq F$ and that $F - F^*$ is countable. The following was proved in KREISEL [1959b].

THEOREM. *The C–B theorem is false in HYP.*

The proof loc. cit. gives a recursively described closed F such that $F - F^*$ consists of HYP reals of arbitrarily large degree, hence which cannot be enumerated by a HYP function. Further, $F^* \cap \text{HYP}$ is empty. Thus, in this model, it is not even true that if a closed set contains no (non-empty) perfect subset, then it is countable.

The following is an example from algebra with related features (FEFERMAN [1975], after an example by Barwise).

THEOREM. *The statement that every Abelian group contains a largest divisible subgroup is false in HYP.*

For this one defines a recursively presented Abelian (p -group) G such that $\bigcup H[H \subseteq G, H \text{ divisible and } H \in \text{HYP}]$ is not in HYP.

7.6.5. Third-order statements

Various statements about sets of reals do not have second-order translations, but relate directly to which reals exist. These may be tested in structures with $M_1 = \text{HYP}$ in which M_2 has a simple description.

THEOREM. *The following statements may be falsified in suitable $\mathfrak{M}$ with $M_1 = \text{HYP}$.*

- (i) *Every set of reals which is closed under limits is closed.*
- (ii) *Every open covering of $[0, 1]$ has a finite subcover.*
- (iii) *There exist analytic non-Borel sets.*
- (iv) *There exist Lebesgue non-measurable sets.*
- (v) *Every set of reals has an outer measure.*

The same $\mathfrak{M}$ suffices for (i)–(iv) but of course not (v).

7.7. Some special ω -models for second-order systems

Next are examples of ω -models which do not appear as the 1-sections of the kind of finite type structures considered above. Each is specified by a

subclass of $\mathbf{N}^{\mathbf{N}}$ or $\mathcal{P}(\mathbf{N})$. The simplest is $\mathcal{H}_{\omega}$ = the collection of arithmetic sets, which forms a model of $(\Pi_1^0 - \text{CA})$. Thus the existence of H_{ω} is not provable in $(\Pi_1^0 - \text{CA})$, though it follows from $(\Delta_1^1 - \text{CA})$. Consider analogously

$$\bar{\mathcal{O}}_1 = \text{Rec}(\mathcal{O}) \quad (1)$$

and

$$\bar{\mathcal{O}}_{\omega} = \text{the collection of sets recursive in some } \mathcal{O}_n. \quad (2)$$

For any scheme S , $(S)^{-}$ indicates the corresponding scheme without second-order parameters. The following were observed by Kreisel.

THEOREM. (i) $\bar{\mathcal{O}}_1$ satisfies $(\Pi_1^1 - \text{CA})^{-}$ but not full $(\Pi_1^1 - \text{CA})$.

(ii) $\bar{\mathcal{O}}_{\omega}$ satisfies $(\Pi_1^1 - \text{CA})$ but not $(\Delta_2^1 - \text{CA})^{-}$.

(iii) $\bar{\mathcal{O}}_1$ is a model of $(\text{BI}_{<})$ for primitive recursive $<$.

(iv) $\bar{\mathcal{O}}_{\omega}$ is a model of (BI) .

PROOF. (i) The positive part is by the Kleene basis theorem. For the negative part argue indirectly: if $(\Pi_1^1 - \text{CA})$ were satisfied, then $\mathcal{O}_2$ would be in $\bar{\mathcal{O}}_1$.

(ii) The positive part uses the basis theorem relativized; for the negative result, note that $\langle \mathcal{O}_n \rangle_{n < \omega}$ is the unique solution of a Σ_2^1 -predicate.

(iii) If $<$ is primitive recursive and has no descending sequences in $\bar{\mathcal{O}}_1$, then it is well-founded and hence TI holds over $<$ with any predicate.

(iv) By relativization of (iii). $\square$

NOTE. The models given are not minimal, since it was shown by Gandy, Kreisel and Tait that the intersection of all ω -models of a recursive (or even Π_1^1) theory is contained in HYP.

7.8. $(\Delta_1^1 - \text{CA})$, $(\Sigma_1^1 - \text{AC})$, $(\Sigma_1^1 - \text{DC})$

KREISEL [1962] proved that HYP is the smallest model of $(\Delta_1^1 - \text{CA})^{-}$, so it cannot be used to distinguish among these three systems. FRIEDMAN [1967, 1970a] showed that $(\Sigma_1^1 - \text{DC})$ is a conservative extension of $(\Pi_1^0 - \text{CA})_{<\epsilon_0}$ and hence also of $(\Delta_1^1 - \text{CA})$, for Π_2^1 -sentences; this will be described in 8.6. He also showed that $(\Sigma_1^1 - \text{DC})$ is a proper extension of $(\Sigma_1^1 - \text{AC})$. STEEL [1974] announced that $(\Sigma_1^1 - \text{AC})$ is a proper extension of $(\Delta_1^1 - \text{CA})$; it is open whether $(\Sigma_1^1 - \text{AC})^{-}$ is derivable from $(\Delta_1^1 - \text{CA})$.

8. Second-order content of the theories studied; proof-theoretical methods

8.1. Introduction

The general problem here is to give precise information about the second-order theorems T^2 of a finite type theory T^ω , and in particular to describe a basis for the Σ_1^1 theorems of T^2 , i.e., a class of functions M_1 such that if $T^2 \vdash \exists f \phi(f)$ with ϕ arithmetical, then $(\exists f \in M_1) \phi(f)$. By *direct* proof-theoretical methods for this problem we mean extensions of Gentzen's *cut-elimination* theorems for *calculi of sequents* (or related *normalization* theorems for *calculi of natural deduction*) to *infinitary* languages following Lorenzen, Schütte, and Tait. Some of the systems considered above can be translated directly into such languages, and the cut-elimination theorem can be used to obtain information about provable well-orderings and Σ_1^1 theorems. A few results obtained in this way are mentioned in 8.2. By *indirect* methods a considerably wider class of theories can be treated. The principal ones here make use of passage through formally intuitionistic theories (8.4) followed by Gödel's *functional interpretation* (8.5) which associates a quantifier-free theory of functionals T_0^ω with given T^ω . Finally, the *terms* of T_0^ω may be analyzed by the method of *normalization*; some basic material for that is given in 8.3. The applications are dealt with in the remainder of Section 8.

8.2. Direct proof-theoretical methods

8.2.1. Infinitary cut-elimination

Since these methods are described in some detail by SCHÜTTE [1960], TAIT [1968], TAKEUTI [1975] and in Chapter D.2, only the relevant conclusions are mentioned. The use of *infinitely long formulas and derivations* is stressed because these are simplifying and make clear the relevance of ordinals. Each such formula ϕ (or derivation d) is a *well-founded tree* and hence has an *ordinal length* denoted by $|\phi|$ (by $|d|$). Using a system for deriving (finite) disjunctions of formulas $\Gamma = (\phi_1 \vee \cdots \vee \phi_n)$, the *cut-rule* may be put in the form

$$(C_\phi) \quad \frac{\Gamma \vee \phi \quad \Gamma \vee \neg \phi}{\Gamma}.$$

d is *cut-free* if no application of this rule occurs in d . The *cut-rank* $\rho(d)$ of a derivation d is defined by

$$\rho(d) = \begin{cases} \sup\{|\phi| + 1 : (C_\phi) \text{ occurs in } d\} & \text{if } d \text{ contains some cut,} \\ 0 & \text{if } d \text{ is cut-free.} \end{cases} \quad (1)$$

The essential feature of the rules of *infinitary predicate calculus* used other than (C) is the *subformula property*: each formula in a hypothesis of the rule is a subformula of some formula in the conclusion. This permits establishing certain properties of cut-free derivations by induction on their length. The main result then is that every derivation d can be transformed into a cut-free derivation d^* . This is proved by a direct extension of Gentzen's argument for first-order predicate calculus. The following form in TAIT [1968] gives a useful measure of the increase in length which d^* may need compared to the length of d .

THEOREM. *If $d \vdash \phi$ with $|d| \leq \beta$ and $\rho(d) \leq \gamma + \omega^\alpha$, then we can find a derivation d^* of ϕ with $|d^*| \leq \kappa^{(\alpha)}(\beta)$ and $\rho(d^*) \leq \gamma$.*

In particular, if d has finite cut-rank $n = \omega^0 \cdot n$, then the n -fold repetition of this result gives cut-free d^* of the same conclusion with $|d^*| < \varepsilon(\beta)$ where $\varepsilon(\beta) = \varepsilon_{\nu+1}$ = the least ε number beyond β ($\varepsilon_\nu \leq \beta < \varepsilon_{\nu+1}$).

8.2.2. The ubiquity of ε_0

Let Z' be Z in a language with additional sorts of variables and full induction for $\mathbb{N}$, but no further new axioms. Z' is translated into an infinitary language, $\phi \mapsto \phi^+$ by taking $(\exists n \phi(n))^+ = \bigwedge_n \phi(\bar{n})^+$. Each derivation $d \vdash \phi$ of Z' may be transformed into a derivation $d^+ \vdash \phi^+$ with $|d^+| < \omega \cdot 2$ and $\rho(d^+) < \omega$. Then any such d transforms to a cut-free derivation d^* of length $< \varepsilon_0$. For formulas ϕ of any given bounded complexity m we can express a truth definition Tr_m in Z' . Then by the subformula property and $\text{TI}(\varepsilon_0)$ we can show that every formula of d^* is true if d proves a formula of complexity $\leq m$. This allows one to establish the so-called *reflection principle* for Z' :

$$Z' + \text{TI}(\varepsilon_0) \vdash \text{Pr}_{Z'}(\ulcorner \phi \urcorner) \rightarrow \phi, \quad (1)$$

where $\text{Pr}_{Z'}(\ulcorner \phi \urcorner)$ expresses that $Z' \vdash \phi$. In particular, if we take $\phi = \neg \psi$, it follows that

$$Z' + \psi + \text{TI}(\varepsilon_0) \vdash \text{Con}_{(Z' + \psi)}. \quad (2)$$

Hence by Gödel's Second Incompleteness Theorem there must be an

instance of $\text{TI}(\varepsilon_0)$ which is not provable in $\mathbf{Z}' + \psi$ if it is consistent. The following strengthening of this result is given in KREISEL and LÉVY [1968].

THEOREM. *Suppose $\mathbf{S}$ is a consistent extension of $\mathbf{Z}'$ by axioms of some bounded complexity; then there is an instance of $\text{TI}(\varepsilon_0)$ which is not provable in $\mathbf{S}$.*

In particular, if $\mathbf{Z}'$ is arithmetic in a second-order or finite type language, every consistent bounded complexity extension of $\mathbf{Z}'$ has an instance of $\text{TI}(\varepsilon_0)$ not provable in it. This applies to such theories as $(\Pi_\infty^0 - \text{CA})$, $(\Sigma_1^1 - \text{DC})$, $(\Pi_1^1 - \text{CA})$, $(\Sigma_2^1 - \text{DC})$, $\mathbf{Z}^\omega + (\exists^*) + (\text{QF} - \text{AC})$, etc. It does not apply to (BI) or $(\text{BI}_<)$ ($<$ primitive recursive).

8.2.3. Ordinal bounds for arithmetical and ramified analysis

To move up to $(\Pi_\infty^0 - \text{CA})$, replace the quantifiers $\forall X \phi(X)$ by $\bigwedge_{\psi \in \mathfrak{A}} \phi(\psi)$ where $\mathfrak{A}$ is the class of arithmetical formulas. Then any finite derivation d of ϕ in $(\Pi_\infty^0 - \text{CA})$ is transformed directly into a derivation d^+ of ϕ^+ where $|d^+| < \omega \cdot 2$ and $\rho(d^+) < \omega \cdot 2$. Applying the theorem of 8.2.1 first to reduce cut-rank from $\omega + n$ to ω , and then from ω to 0 one obtains cut-free d^* with $|d^*| < \varepsilon_{\varepsilon_0}$.

THEOREM. $(\Pi_\infty^0 - \text{CA}) \not\vdash I(\varepsilon_{\varepsilon_0})$.

Ordinal bounds for the ramified systems RA_α may be obtained similarly. The simplest description is when α is an ε -number.

THEOREM. *If $\omega^\alpha = \alpha$, then $\text{RA}_\alpha \not\vdash I(\kappa^{(\alpha)}(0))$.*

From this one obtains that induction up to Γ_0 (the least solution of $\kappa^{(\alpha)}(0) = \alpha$) is not provable in an autonomous progression of ramified theories (cf. 6.4.5).

8.3. Normalization of infinite terms

8.3.1. The terms and reduction procedures

We here follow TAIT [1965] in considering terms built up from variables of finite type and 0 by successor, application, *abstraction* $(\lambda a.t)$ and *sequencing* $(\langle t_n \rangle_n)$. These may be treated similarly to infinite derivations, and have certain technical advantages compared to the use of combinators and recursion operators; the latter are replaced by infinite terms as follows (for each appropriate combination of types):

$$R \mapsto R^+ = \lambda f \lambda a \langle t_n \rangle_n, \quad \text{where } t_0 = a, \quad t_{n+1} = f 0^{(n)} t_n. \quad (1)$$

Again, each term t is a well-founded tree and has a length $|t|$. Replacing the combinators K and S by $\lambda a \lambda b. a$ and $\lambda f \lambda g \lambda a. fa(ga)$, respectively, each ordinary term t is sent into an infinitary λ -term t^+ with $|t^+| < \omega \cdot 2$. In general, the following simplifications or *immediate reductions* may be applied to infinitary terms (reading ' $\equiv$ ' as 'reduces to'):

$$(\equiv_1) \quad (\lambda a. t[a])s \equiv t[s],$$

where $t[s] = \text{subst}(s/a)t$.

$$(\equiv_2) \quad \langle t_n \rangle_n 0^{(m)} \equiv t_m.$$

$$(\equiv_3) \quad \langle t_n \rangle_n r s \equiv \langle t_n s \rangle_n r.$$

The last is applied only when $\langle t_n \rangle_n r$ is not of type 0 and r is not a numeral $0^{(n)}$. Consider the least transitive and reflexive relation $\equiv$ which contains $\equiv_i$ ($i = 1, 2, 3$) and preserves application. If $t \equiv s$, then t and s define the same object at any common assignment to their free variables. We say that t is *irreducible* or *normal* if $t \equiv s$ implies $t = s$, i.e., if t has no immediately reducible subterms. Such subterms have a *cut-complexity* analogous to that for the cut-rule; e.g., the complexity of $(\lambda a t[a])s$ is $\text{lev}(\text{type}(a))$. Then $\rho(t)$ is defined as the least ordinal greater than all such complexities in t . Note that $\rho(t^+) < \omega$ for t an ordinary term. In analogy to the cut-elimination theorem of 6.2.1, TAIT [1965] obtained a *normalization theorem*, of which we need only the following special result.

THEOREM. *Suppose $\rho(t) < \omega$ and $|t| < \varepsilon_0$; then we can find t^* in n.f. with $t \equiv t^*$ and $|t^*| < \varepsilon_0$.*

The proof is similar to that for derivations.

8.3.2. Normal terms of type 0

Every term t of type 1 defines the same function as $\lambda n. tn$. Thus for a study of such it is sufficient to consider normal terms of type 0. If t is of type 0 and normal and contains only numerical free variables, then either

- (i) $t = 0$ or
- (ii) $t = s'$ where s is normal or
- (iii) t is a variable of type 0 or
- (iv) $t = \langle t_n \rangle_n s$ where each t_n and s is normal of type 0 but s is not a numeral.

It follows that the only closed terms of type 0 are numerals. Suppose now

that t is normal and contains only variables of type 0, 1, 2 free. Then either (i)–(iv) or

(v) $t = f^1(s)$ where f is a type 1 variable, and s is normal of type 0, or

(vi) $t = f^2(\lambda n. s)$ where f^2 is a type 2 variable and s is normal of type 0, or finally

(vii) $t = f^2(\langle t_n \rangle_n)$ where each t_n is normal of type 0.

Thus again we have a complete generation of the normal terms of type 0.

8.3.3. The 1-section of (relative) primitive recursion

Let **PR** be Gödel's primitive recursive functionals of finite type, i.e., those defined by terms generated from 0, Sc, using all K , S , and R 's. For F of type 2, $\mathbf{PR}(F)$ denotes the class generated using F as well. Let $\text{REC}_{<\varepsilon_0}$ consist of the functions of type 1 defined by ordinary primitive recursion and transfinite recursion on any $<_\alpha$ for $\alpha < \varepsilon_0$. The following is in TAIT [1965].

THEOREM. $1\text{-sec}(\mathbf{PR}) = \text{REC}_{<\varepsilon_0}$.

PROOF. By 8.3.1 each element of $1\text{-sec}(\mathbf{PR})$ is denoted by an effectively given infinite λ -term of the form $\lambda n. t$ where t is normal of type 0 with at most ' n ' free, and $|t| < \varepsilon_0$. Then the value of t at n , $\text{Val}(t, n)$ is defined by recursion on the length of t . $\square$

Next, using Shoenfield's hierarchy H_a^F and the classes $\mathcal{H}_a^F$ of functions recursive in some H_a^F with $|a| < \varepsilon_0$, we obtain analogously (FEFERMAN [1971]):

THEOREM. $1\text{-sec}(\mathbf{PR}(F)) = \mathcal{H}_{\varepsilon_0}^F$.

PROOF. Each element of $1\text{-sec}(\mathbf{PR}(F))$ is denoted by some effectively given term $\lambda n. t$ where t contains at most n, f^2 free where f^2 denotes F , t is normal of type 0, and $|t| < \varepsilon_0$. Following the build-up of 8.3.2 we see that the function defined by $\lambda n. t$ is recursive in H_a^F where $|a| = |t|$. $\square$

COROLLARY. $1\text{-sec}(\mathbf{PR}(\mu)) = 1\text{-sec}(\mathbf{PR}(\exists^N)) = \mathcal{H}_{\varepsilon_0}$.

8.3.4. The 1-section of relative elementary primitive recursion

$\hat{\mathbf{PR}}(F)$ is described in the same way as $\mathbf{PR}(F)$ except we use the operators $\hat{R}$ instead of R .

THEOREM. *Suppose $\exists^N$ is recursive in F ; then $1\text{-sec}(\widehat{\mathbf{PR}}(F)) = \mathcal{H}_\omega^F$.*

PROOF (FEFERMAN [1971]). The relation $\hat{R}fanb = m$ is arithmetically definable in f, a, n, b, m since we need only talk about finite sequences of type 0 objects. Thus, every member of $\widehat{\mathbf{PR}}(F)$ is definable by a finite λ -term without sequencing but with $+$ and $\cdot$, and with at most f^2 free. Normalization of these takes place in the finite λ -calculus. $\square$

COROLLARY. $1\text{-sec}(\widehat{\mathbf{PR}}(\mu)) = 1\text{-sec}(\widehat{\mathbf{PR}}(\exists^N)) = \text{the arithmetic functions.}$

8.4. Passage to formally intuitionistic systems

8.4.1. The negative translation

With each classical theory T considered below we associate a formally intuitionistic theory $(T)^i$ by dropping the law of excluded middle (LEM) from its basic logic (since it is generally easier to analyze the explicit content of $(T)^i$). LEM is retained for atomic formulas. We emphasize the adjective “formally”, since the systems which contain functionals such as $\exists^N$ or $\exists \downarrow^N$, etc. do not express intuitionistic principles. In 1933 Gödel gave a simple translation of classical number theory $\mathbf{Z}$ into intuitionistic number theory $\mathbf{HA}$ (“Heyting’s Arithmetic”) which extends directly to a translation of $\mathbf{T}$ into $(T)^i$ for many of the $\mathbf{T}$ considered here. This sends each ϕ into a formula $(\phi)^i$ where $(\)^i$ preserves atomic formulas and the operations $\wedge$, $\rightarrow$ and $\forall$ while

$$(\phi \vee \psi)^i = \neg(\neg(\phi)^i \wedge \neg(\psi)^i), \quad (1)$$

$$(\exists a \phi)^i = \neg \forall a \neg(\phi)^i. \quad (2)$$

Equivalently, one can take $(\phi \vee \psi)^i$ to be $\neg \neg [(\phi)^i \vee (\psi)^i]$ and $(\exists a \phi)^i$ to be $\neg \neg \exists a (\phi)^i$. Further details on this so-called *negative* (or *double-negation*) translation may be found in Chapter D.5, 3.8–3.10.

THEOREM. *If $\mathbf{T}$ is an $(\vee, \exists)$ -free extension of $\mathbf{Z}^\omega$, i.e., by (possibly) additional constants and by axioms which do not contain disjunctions or existential quantifiers, then $\mathbf{T}$ is translated into $(\mathbf{T})^i$.*

The system $(\mathbf{Z}^\omega)^i$ is denoted $\mathbf{HA}^\omega$.

8.4.2. Extensions by some selection operators

The theorem of 8.4.1 can be applied to $\mathbf{Z}^\omega + (\exists^N)$ by slight modification of the additional axiom. However, for purposes below we apply it instead

to the classically equivalent system $\mathbf{Z}^\omega + (\mu)$ where the unbounded minimum operator μ (of type 2) is adjoined with the axiom

$$(\mu) \quad fn = 0 \rightarrow f(\mu f) = 0 \wedge \mu f \leq n.$$

Note that the definition: $\exists^\mathbf{N} f = [0 \text{ if } f(\mu f) = 0, 1 \text{ otherwise}]$ works with intuitionistic logic as well so $\mathbf{HA}^\omega + (\mu)$ is equivalent to $\mathbf{HA}^\omega + (\exists^\mathbf{N})$. $\mathbf{Z}^\omega + (\mu)$ is translated directly into $\mathbf{HA}^\omega + (\mu)$. The latter system is certainly not intuitionistic (constructive) since we can prove $\exists n (fn = 0) \vee \neg \exists n (fn = 0)$ from $f(\mu f) = 0 \vee f(\mu f) \neq 0$; more generally LEM holds for any arithmetical formula.

Similarly, for purposes below with $\mathbf{Z}^\omega + (\exists \downarrow^\mathbf{N})$ we pass through $\mathbf{Z}^\omega + (L)$ where L is the leftmost branch selection operator having the $(\vee, \exists)$ -free axiom:

$$(L) \quad \forall n f(\bar{g}(n)) = 0 \rightarrow \forall n f(\overline{Lf}(n)) = 0 \wedge Lf0 \leq g0.$$

COROLLARY. (i) $\mathbf{Z}^\omega + (\mu)$ is reduced to $\mathbf{HA}^\omega + (\mu)$ by the negative translation.

(ii) $\mathbf{Z}^\omega + (L)$ is reduced to $\mathbf{HA}^\omega + (L)$ by the negative translation.

8.5. Gödel's functional interpretation and its applications to $\mathbf{Z}^\omega$

8.5.1. Form of the interpretation

This was given originally by GÖDEL [1958] for $\mathbf{HA}$ but applied immediately to $\mathbf{HA}^\omega$. For full details cf. Section 11 of Chapter D.5; we need to know the following only. With each formula ϕ of the language of $\mathbf{HA}^\omega$ is associated a formula ϕ^D ('D' for 'Dialectica') with the same free variables as ϕ .

$$\phi^D = \exists \mathbf{a} \forall \mathbf{b} \phi_D(\mathbf{a}, \mathbf{b}) \quad (1)$$

where $\mathbf{a}, \mathbf{b}$ are (possibly empty) sequences of variables of various types determined by ϕ ; further, ϕ_D is quantifier-free. Special cases in the inductive definition of ϕ^D are

$$(\forall c \phi)^D = \exists f \forall c, \mathbf{b} \phi_D(fc, \mathbf{b}), \quad (2)$$

$$(\neg \phi)^D = \exists g \forall \mathbf{a} \neg \phi_D(\mathbf{a}, g\mathbf{a}). \quad (3)$$

In particular, if the list $\mathbf{b}$ is empty, $(\neg \phi)^D = \forall \mathbf{a} \neg \phi_D(\mathbf{a})$ and $(\neg \neg \phi)^D = \exists \mathbf{a} \neg \neg \phi_D(\mathbf{a})$ which is equivalent to $\exists \mathbf{a} \phi_D(\mathbf{a})$ since atomic formulae are decided

COROLLARY. (i) If ϕ is existential, then $(\phi^i)^D$ is equivalent to ϕ .

- (ii) If $\phi = \forall a \exists b \theta(a, b)$ with θ quantifier-free, then $(\phi^i)^D$ is equivalent to $\exists f \forall a \theta(a, fa)$.
- (iii) $((QF - AC)^i)^D$ is logically valid.

8.5.2. Interpretation of $\mathbf{HA}^\omega$ and $\mathbf{Z}^\omega$

Let $QF - \mathbf{HA}^\omega$ be the quantifier-free part of $\mathbf{HA}^\omega$; this may be axiomatized in a straightforward way as the theory of primitive recursive functionals. Thus we denote it by $\mathbf{PR}^\omega$ (usually referred to as “Gödel’s $\mathbf{T}''$). Gödel’s argument shows (GÖDEL [1958]):

THEOREM. *If $\mathbf{HA}^\omega \vdash \phi$ and $\phi^D = \exists a \forall b \phi_D(a, b)$, then for some sequence t of terms $\mathbf{PR}^\omega \vdash \phi_D(t, b)$.*

COROLLARY 1. *If $\mathbf{Z}^\omega + (QF - AC) \vdash \forall a \exists b \theta(a, b)$ with θ quantifier-free, then $\mathbf{PR}^\omega \vdash \theta(a, ta)$ for some term t .*

Each term t denotes a member of $\mathbf{PR}$; by 8.3.3 one obtains the following result due to Kreisel (cf. Chapter D.2).

COROLLARY 2. *The provably recursive functions of $\mathbf{Z}^\omega$ form exactly the class $\text{REC}_{<\varepsilon_0}$.*

We shall obtain analogous results for theories with selection functionals.

8.6. Non-constructive extensions of the functional interpretation

8.6.1. General statement

The following is obtained by applying the negative translation followed by the Dialectica interpretation.

THEOREM. *Suppose ψ does not contain $\vee$ or quantifiers but (possibly) additional constants. Then $\mathbf{Z}^\omega + \psi + (QF - AC)$ is Dialectica-interpreted in $\mathbf{PR}^\omega + \psi$.*

8.6.2. Application to adjunction of $(\exists^\mathbf{N})$ and (μ)

As a corollary to the preceding theorem and 8.5 we have:

THEOREM. *If $\mathbf{Z}^\omega + (\mu) + (QF - AC) \vdash \forall a \exists b \theta(a, b)$ with θ quantifier-free, then $\mathbf{PR}^\omega + (\mu) \vdash \theta(a, t[a])$ for some term t of $\mathbf{PR}(\mu)$.*

THEOREM. (i) If $\mathbf{Z}^\omega + (\mu) + (\mathbf{QF} - \mathbf{AC}) \vdash \exists f^1 \theta(f)$ with θ arithmetical, then $\theta(f)$ is true for some f in $\mathcal{H}_{\varepsilon_0}$.

(ii) $\mathbf{Z}^\omega + (\mu) + (\mathbf{QF} - \mathbf{AC})$ is a conservative extension of $(\Pi_1^0 - \mathbf{CA})_{<\varepsilon_0}$ for Π_2^1 sentences.

PROOF. (i) θ is equivalent to a quantifier-free formula using (μ) . One then applies the preceding theorem and the result of 8.3.3 that $1\text{-sec}(\mathbf{PR}(\mu)) = \mathcal{H}_{\varepsilon_0}$.

(ii) Consider a Π_2^1 sentence $\forall f \exists g \theta(f, g)$ with θ arithmetical, provable in $\mathbf{Z}^\omega + (\mu) + (\mathbf{AF} - \mathbf{AC})$. There is a term $t[f]$ in $\mathbf{PR}(\mu)$ with $\theta(f, t[f])$ provable in $\mathbf{PR}^\omega + (\mu)$. By 8.3.3 we have $t[f] \in \mathcal{H}_{\varepsilon_0}^f$ uniformly in f , so for some $\alpha < \varepsilon_0$, $t[f] \in \mathcal{H}_\alpha^f$ uniformly in f . For $|a| = \alpha$ and variable f the existence of H_a^f can be proved in $(\Pi_1^0 - \mathbf{CA})_{<\varepsilon_0}$. The argument is completed by formalization. $\square$

Since $(\Sigma_1^1 - \mathbf{DC})$ is contained in $\mathbf{Z}^\omega + (\exists^\omega) + (\mathbf{QF} - \mathbf{AC})$, we obtain:

COROLLARY. (i) $(\Sigma_1^1 - \mathbf{DC})$ is a conservative extension of $(\Pi_1^0 - \mathbf{CA})_{<\varepsilon_0}$ for Π_2^1 -sentences.

(ii) $\kappa^{(\varepsilon_0)}(0)$ is the sup of the provably recursive well-orderings of $(\Sigma_1^1 - \mathbf{DC})$.

This result is due to FRIEDMAN [1967]; the nature of his proof, which is also presented in FRIEDMAN [1970a], will be discussed in the next section. The present proof via the Dialectica interpretation (allowing improvement to finite type theories) was presented in FEFERMAN [1971].

NOTE. (i) tells us that $(\Sigma_1^1 - \mathbf{DC})$ is reducible to predicative principles though it is *prima-facie* impredicative (and its least ω -model $\mathbf{HYP}$ is certainly impredicative).

8.6.3. Application to adjunction of $(\exists \downarrow^\omega)$ and (L)

We obtain by the same lines of argument:

THEOREM. If $\mathbf{Z}^\omega + (L) + (\mathbf{QF} - \mathbf{AC}) \vdash \forall a \exists b \theta(a, b)$ with θ quantifier-free, then $\mathbf{PR}^\omega + (L) \vdash \theta(a, t[a])$ for some term t of $\mathbf{PR}(L)$.

THEOREM. $\mathbf{Z}^\omega + (L) + (\mathbf{QF} - \mathbf{AC})$ is a conservative extension of the theory $(\Pi_1^1 - \mathbf{CA})_{<\varepsilon_0}$ for Π_3^1 sentences.

Note for the latter that $\mathcal{H}_{\varepsilon_0}^L$ is just a form of the hyperjump hierarchy up to ε_0 . This gives another result of FRIEDMAN [1970a]:

COROLLARY. $(\Sigma_2^1 - DC)$ is a conservative extension of $(\Pi_1^1 - CA)_{<\varepsilon_0}$ for Π_3^1 sentences.

NOTE. The idea of Friedman's proof of 8.6.2 Corollary (i) is not easy to explain succinctly, and the following only indicates its pattern. Suppose ψ is in Σ_2^1 and is consistent with $(\Pi_1^0 - CA)_{<\varepsilon_0}$; it is to be shown that ψ is consistent with $(\Sigma_1^1 - DC)$. We know by 8.2.2 that there is an instance $TI(\varepsilon_0, \phi)$ of transfinite induction up to ε_0 which is not provable in $(\Pi_1^0 - CA)_{<\varepsilon_0} + \psi$. One may try to model $(\Sigma_1^1 - DC) + \psi$ in $(\Pi_1^0 - CA)_{<\varepsilon_0} + \psi + \neg TI(\varepsilon_0, \phi)$ via the set of functions recursive in some H_α with $\phi(\alpha)$. That does not quite work, since some portion of the scheme $TI(\varepsilon_0)$ must still be used to verify the properties of the model. However, the proof can be carried through by certain modifications of this idea. It is evidently one of its features that non-standard models play a principal role; this is to be expected of any model-theoretic argument, since HYP is the least standard model of $(\Sigma_1^1 - DC)$. By similar arguments, FRIEDMAN [1970a] obtained the corollary above for $(\Sigma_2^1 - DC)$ and further such results for $(\Sigma_k^1 - AC)$ when $k > 2$.

Another proof of the corollary in 8.6.2 above for $(\Sigma_1^1 - DC)$ was given by TAIT [1968] using cut-elimination methods following those of 8.2; extension to $(\Sigma_2^1 - DC)$ is dealt with in TAIT [1970].

Still another proof of the corollary in 8.6.2 was given by HOWARD [1968] using a constructive Dialectica interpretation with so-called bar recursion; cf. Chapter D.5, Section 11.

8.6.4. Conservative extensions of systems for absolute hierarchies

Given a definable functional F on subsets of $\mathbb{N}$, let $\text{Hier}_<^F(X)$ be the formula $\text{Hier}_<^F(X, \mathbb{N})$ of 6.4.1 expressing that X is a hierarchy for F along $<$ starting with $X_0 = \mathbb{N}$; such sets X may be called *absolute hierarchies* for F . Using the jump and hyperjump operators J and J_1 , write $(\Pi_1^0 - CA)_\alpha^-$ for $\exists X \text{Hier}_<_\alpha^J(X)$ and $(\Pi_1^1 - CA)_\alpha^-$ for $\exists X \text{Hier}_<_\alpha^{J_1}(X)$. Then, as before, $(\Pi_1^1 - CA)_{<\alpha}^-$ denotes the collection of statements $(\Pi_1^1 - CA)_\beta^-$ for all $\beta < \alpha$. Note that $(\Delta_{i+1}^1 - CA)^- \supseteq (\Pi_1^1 - CA)_{<\varepsilon_0}^-$ for $i = 0, 1$.

The conservation results of 8.6.2, 8.6.3 may be strengthened by replacing $(\Pi_1^1 - CA)_{<\varepsilon_0}$ by $(\Pi_1^1 - CA)_{<\varepsilon_0}^-$ but only at the cost of decreasing the class of statements conserved

THEOREM. (i) $Z^\omega + (\mu) + (QF - AC)$ is a conservative extension of $(\Pi_1^0 - CA)_{<\varepsilon_0}^-$ for Σ_1^1 sentences.

(ii) $Z^\omega + (L) + (QF - AC)$ is a conservative extension of $(\Pi_1^1 - CA)_{<\varepsilon_0}^-$ for Σ_2^1 sentences.

The proofs require no essentially new points besides those indicated above. For example, in the case of (i) we have seen that if $\mathbf{Z}^\omega + (\mu) + (\text{QF} - \text{AC}) \vdash \exists b \theta(b)$ with θ arithmetical, then for some $\alpha < \varepsilon_0$ and $f \in \mathcal{H}_\alpha$, $\theta(f)$ is true. H_α can be proved to exist in $(\Pi_1^0 - \text{CA})_{<\varepsilon_0}^-$. The argument then proceeds by formalization of these observations.

COROLLARY. (i) $(\Sigma_1^1 - \text{DC})$ is a conservative extension of $(\Pi_1^0 - \text{CA})_{<\varepsilon_0}^-$ (and hence of $(\Delta_1^1 - \text{CA})^-$) for Σ_1^1 sentences.

(ii) $(\Sigma_2^1 - \text{DC})$ is a conservative extension of $(\Pi_1^1 - \text{CA})_{<\varepsilon_0}^-$ (and hence of $(\Delta_2^1 - \text{CA})^-$) for Σ_2^1 sentences.

Part (i) of this corollary was obtained in KREISEL [1975], Appendix 2; his argument adapts (and elaborates) that of FRIEDMAN [1970a].

NOTE. As Kreisel remarks (see KREISEL [1975]), if $(\Pi_1^0 - \text{CA})_\alpha^- \vdash I(\beta)$ where $\alpha < \omega_1$, then $\beta < \varepsilon_0$. This follows from the general result of KREISEL [1968], p. 341 that if $\mathbf{T}$ is an extension of $\mathbf{Z}^2$ by true Σ_1^1 sentences, then $\beta < \varepsilon_0$ whenever $\mathbf{T} \vdash I(\beta)$.

8.7. Systems with restricted induction

We shall use the method above to improve the result of 5.5.1. In verifying the Dialectica interpretation of restricted induction I^N it is only necessary to use the operator $\hat{R}$.

THEOREM. If restricted $(\mathbf{Z}^{(\omega)}) + (\mu) + (\text{QF} + \text{AC}) \vdash \forall a \exists b \theta(a, b)$ where θ is quantifier-free, then $\widehat{\mathbf{PR}}^{(\omega)} + (\mu) \vdash \theta(a, t[a])$ for some term t , where $\widehat{\mathbf{PR}}^{(\omega)}$ is the quantifier-free part of restricted $(\hat{\mathbf{Z}}^{(\omega)})$.

By 8.3.4, $1\text{-sec}(\mathbf{PR}(\mu))$ = the arithmetic functions. Hence if the system considered proves a Σ_1^1 sentence, that sentence is true in the structure of arithmetic functions. Further, by formalizing the argument needed for any particular derivation from the system, one obtains:

THEOREM. Restricted $(\hat{\mathbf{Z}}^{(\omega)}) + (\mu) + (\text{QF} - \text{AC})$ is a conservative extension of $\mathbf{Z}$.

COROLLARY. Restricted $(\Sigma_1^1 - \text{AC})$ is a conservative extension of $\mathbf{Z}$.

Note that the method does not work for restricted $(\Sigma_1^1 - \text{DC})$, since to

derive that from higher-type (QF – AC) with (μ) we need the recursion operators R .

Note. The above theorems and corollary improve conservation results over $\mathbf{Z}$ by (i) BARWISE and SCHLIPF [1975] and independently by FRIEDMAN [1975] induction and arithmetical comprehension. One can also obtain a result for restricted $\hat{\mathbf{Z}}^\omega + (L) + (\text{QF} - \text{AC})$ and hence restricted $(\Sigma_2^1 - \text{AC})$ over restricted $(\Pi_1^1 - \text{CA})$.

9. Sources for further topics

9.1. Methods and applications of proof theory

- (i) Basic papers (GENTZEN [1969]),
- (ii) texts (SCHÜTTE [1960], TAKEUTI [1975]),
- (iii) survey of methods and applications to systems of analysis (KREISEL [1968]),
- (iv) systems of natural deduction and normalization (PRAWITZ [1971]).

9.2. Systems of ordinal notations

- (i) Systems based on structures of ordinal functions (FEFERMAN [1968]),
- (ii) systems employing higher number classes after Bachmann (BRIDGE [1975], BUCHHOLZ [1975]),
- (iii) ordinal diagrams (TAKEUTI [1975]).

9.3. Predicativity

Characterizations by Schütte and Feferman in terms of autonomous ramified progressions; equivalent unramified theories (FEFERMAN [1977]).

9.4. Theories of generalized inductive definitions

- (i) One inductive definition (HOWARD [1972]),
- (ii) iterated inductive definitions (FEFERMAN [1970], ZUCKER [1973]).

9.5. Formal theories of ordinals and their functional interpretations

- (i) A constructive theory of countable ordinals (HOWARD [1972]),
- (ii) theories of higher number classes (ZUCKER [1973]).

9.6. Continuous functional interpretations of analysis

- (i) Basic notions and varieties of interpretations (KREISEL [1959a]),
- (ii) bar-recursive functional interpretations (SPECTOR [1962], HOWARD [1968], LUCKHARDT [1973]).

9.7. Functional interpretations with variable types (GIRARD [1971])

References

- BARWISE, J. and J. SCHLIPF
- [1975] On recursively saturated models of arithmetic in: *Model Theory and Algebra: A Memorial Tribute to Abraham Robinson*, edited by D. Saracino and V.B. Weispfennig, Lecture Notes in Mathematics Vol. 498 (Springer, Berlin) pp. 42–55.
- BISHOP, E.
- [1967] *Foundations of Constructive Analysis* (McGraw-Hill, New York).
- BRIDGE, J.
- [1975] A simplification of the Bachmann method for generating large countable ordinals, *J. Symbolic Logic*, **40**, 171–185.
- BUCHHOLZ, W.
- [1975] Normalfunktionen und konstruktive Systeme von Ordinalzahlen. in: *Proof Theory Symposium, Kiel 1974*, edited by J. Diller and G.H. Müller, Lecture Notes in Mathematics Vol. 500 (Springer, Berlin) pp. 4–25.
- CHURCH, A.
- [1940] A formulation of the simple theory of types, *J. Symbolic Logic*, **5**, 56–68.
- FEFERMAN, S.
- [1968] Systems of predicative analysis, II: Representations of ordinals, *J. Symbolic Logic*, **33**, 193–219.
 - [1970] Formal theories for transfinite iterations of generalized inductive definitions and some subsystems of analysis, in: *Intuitionism and Proof Theory*, edited by A. Kino, J. Myhill and R.E. Vesley (North-Holland, Amsterdam) pp. 303–326.
 - [1971] Ordinals and functionals in proof theory, in: *Proceedings of the International Congress of Mathematics, Nice, 1970*, Vol. 1 (Gauthier-Villars, Paris) pp. 229–233.
 - [1975] Impredicativity of the existence of the largest divisible subgroup of an Abelian p -group, in: *Model Theory and Algebra: A Memorial Tribute to Abraham Robinson*, edited by D. Saracino and V.B. Weispfennig, Lecture Notes in Mathematics Vol. 498 (Springer, Berlin) pp. 117–130.
 - [1977] A more perspicuous formal system for predicativity, in: *Lorenzen Festschrift*, to appear.
 - [1978] *Explicit Content of Actual Mathematical Analysis*, Perspectives in Mathematical Logic (Springer, Berlin), to appear.
- FEFERMAN, S. and C. SPECTOR
- [1962] Incompleteness along paths in progressions of theories, *J. Symbolic Logic*, **27**, 383–390.
- FRIEDMAN, H.
- [1967] Subsystems of set-theory and analysis, Dissertation, Massachusetts Institute of Technology, Cambridge, MA.
 - [1969] Bar induction and Π_1^1 -CA, *J. Symbolic Logic*, **34**, 353–362.

- [1970a] Iterated inductive definitions and Σ_1^1 -AC, in: *Intuitionism and Proof Theory*, edited by A. Kino, J. Myhill and R.E. Vesley (North-Holland, Amsterdam) pp. 435-442.
 - [1970b] Higher set theory and mathematical practice, *Ann. Math. Logic*, **2**, 325-357.
 - [1971] Axiomatic recursive function theory, in: *Logic Colloquium '69*, edited by R.O. Gandy and C.M.E. Yates (North-Holland, Amsterdam) pp. 113-138.
 - [1975] Systems of second-order arithmetic with restricted induction, preprint.
- GANDY, R.O.
- [1960] Proof of Mostowski's conjecture, *Bull. Acad. Polon. Sci.*, **8**, 571-575.
 - [1967] General recursive functions of finite type and hierarchies of functionals, *Ann. Fac. Sci. Univ. Clermont-Ferrand* **4**, 5-24.
- GENTZEN, G.
- [1969] *The Collected Papers of Gerhard Gentzen*, edited by M.E. Szabo (North-Holland, Amsterdam).
- GIRARD, J.-Y.
- [1971] Une extension de l'interprétation de Gödel à l'analyse et son application à l'élimination des coupures, in: *Proceedings of the Second Scandinavian Logic Symposium*, edited by J.E. Fenstad (North-Holland, Amsterdam) pp. 63-92.
- GÖDEL, K.
- [1958] Über eine bisher noch nicht benutzte Erweiterung des finiten Standpunktes, *Dialectica*, **12**, 280-287.
- GRZEGORCZYK, A.
- [1955] Elementarily definable analysis, *Fund. Math.*, **41**, 311-338.
- HARRISON, J.
- [1968] Recursive pseudo-well-orderings, *Trans. Am. Math. Soc.*, **131**, 526-543.
- HILBERT, D. and P. BERNAYS
- [1939] *Grundlagen der Mathematik, II* (Springer, Berlin, 2nd. ed. 1970).
- HOWARD, W.A.
- [1968] Functional interpretation of bar induction by bar recursion, *Compositio Math.*, **20**, 107-124.
 - [1972] A system of abstract constructive ordinals, *J. Symbolic Logic*, **37**, 355-374.
- KLEENE, S.C.
- [1959a] Quantification of number-theoretic functions, *Compositio Math.*, **14**, 23-40.
 - [1959b] Countable functionals, in: *Constructivity in Mathematics*, edited by A. Heyting (North-Holland, Amsterdam) pp. 81-100.
 - [1959c] Recursive functionals and quantifiers of finite types, I, *Trans. Am. Math. Soc.*, **91**, 1-52.
- KREISEL, G.
- [1959a] Interpretation of analysis by means of constructive functionals of finite type, in: *Constructivity in Mathematics*, edited by A. Heyting (North-Holland, Amsterdam) pp. 101-128.
 - [1959b] Analysis of the Cantor-Bendixson theorem by means of the analytic hierarchy, *Bull. Acad. Polon. Sci.*, **7**, 621-626.
 - [1962] The axiom of choice and the class of hyperarithmetic functions, *Indag. Math.*, **24**, 307-319.
 - [1968] A survey of proof theory, *J. Symbolic Logic*, **33**, 321-388.
 - [1975] Wie die Beweistheorie zu ihren Ordinalzahlen kam und kommt, text of lecture at meeting of the German Math. Soc., Tübingen, Sept. 1975.
- KREISEL, G. and A. LÉVY
- [1968] Reflection principles and their use for establishing the complexity of axiomatic systems, *Z. Math. Logik Grundlagen Math.*, **14**, 97-142.

LORENZEN, P.

[1951] Mass und Integral in der konstruktiven Analysis, *Math. Z.*, **54**, 275–290.

[1965] *Differential und Integral, eine konstruktive Einführung in die klassische Analysis* (Akad. Verlag, Frankfurt a. M.).

LUCKHARDT, H.

[1973] *Extensional Gödel Functional Interpretation. A Consistency Proof of Classical Analysis*, Lecture Notes in Mathematics, Vol. 306 (Springer, Berlin).

MARTIN, D.A.

[1975] Borel determinacy, *Ann. of Math.*, **102**, 363–371.

PRAWITZ, D.

[1971] Ideas and results in proof theory, in: *Proceedings of the Second Scandinavian Logic Symposium*, edited by J.E. Fenstad (North-Holland, Amsterdam) pp. 235–307.

ROGERS, H.

[1967] *Theory of Recursive Functions and Effective Computability* (McGraw-Hill, New York).

SCHÜTTE, K.

[1960] *Beweistheorie* (Springer, Berlin).

SHOENFIELD, J.R.

[1968] A hierarchy based on a type 2 object, *Trans. Am. Math. Soc.*, **134**, 103–108.

SPECKER, E.

[1971] Ramsey's theorem does not hold in recursive set theory, in: *Logic Colloquium '69*, edited by R.O. Gandy and C.E.M. Yates (North-Holland, Amsterdam) pp. 439–442.

SPECTOR, C.

[1962] Provably recursive functionals of analysis, in: *Recursive Function Theory*, edited by J. Dekker, Proceedings of symposia in pure mathematics, Vol. 5 (Am. Math. Soc., Providence, RI) pp. 1–27.

STEEL, J.

[1974] Forcing with tagged trees, *Notices Am. Math. Soc.*, **21**, A627.

TAIT, W.W.

[1965] Infinitely long terms of transfinite type, in: *Formal Systems and Recursive Functions*, edited by J.N. Crossley and M.A.E. Dummett (North-Holland, Amsterdam) pp. 176–185.

[1968] Normal derivability in classical logic, in: *The Syntax and Semantics of Infinitary Languages*, edited by J. Barwise, Lecture Notes in Mathematics, Vol. 72 (Springer, Berlin) pp. 204–236.

[1970] Applications of the cut-elimination theorem to some sub-subsystems of classical analysis, in: *Intuitionism and Proof Theory*, edited by A. Kino, J. Myhill and R.E. Vesley (North-Holland, Amsterdam) pp. 475–488.

TAKEUTI, G.

[1973] A conservative extension of Peano arithmetic, unpublished.

[1975] *Proof Theory* (North-Holland, Amsterdam).

ZUCKER, J.I.

[1973] Iterated inductive definitions, trees and ordinals, in: *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*, Lecture Notes in Mathematics, Vol. 344 (Springer, Berlin) pp. 392–453.

Aspects of Constructive Mathematics

A.S. TROELSTRA*

Contents

1. Introduction	974
2. Logic	977
3. Some languages, formal systems and notations; the Gödel negative translation	982
4. Realizability and Church's thesis	986
5. Some elementary mathematics	992
6. Continuity; choice sequences	1004
7. Lawless sequences	1019
8. Markov's principle	1021
9. Truth-value semantics for intuitionistic logic; validity in all structures	1024
10. Finite type structures	1026
11. The Dialectica interpretation	1032
12. Local and global constructivizations of classical theorems	1040
References	1047

* The author is indebted to G. E. Minc for information concerning Russian constructivism, and to G. Kreisel for criticism of an earlier draft of this paper.

1. Introduction

1.1. “Constructive” in the title of this chapter is meant in a wide sense and includes such trends or schools as

(a) finitism (HILBERT and BERNAYS [1934, §2c]; KREISEL and KRIVINE [1966, App. IIB]);

(b) constructive recursive analysis CRA, by which we mean constructive mathematics in the sense of ŠANIN [1958, 1964, 1974]; MARKOV [1962, 1971, 1974];

(c) intuitionism (in the sense of BROUWER [1949, 1952, 1954]; HEYTING [1956]; TROELSTRA [1969]);

(d) constructivism in the narrow sense (e.g. BISHOP [1967]) which may be described as intuitionism without choice sequences and without Church’s thesis.

1.2. In this chapter, we approach constructivism as the study of a special area in the whole of mathematical experience. Certain aspects (“phenomena” or “issues”) appear naturally in connection with this study; here we are primarily concerned with such aspects as have mathematical consequences. We do not attempt the systematic development of one particular philosophy of mathematics, nor a detailed comparison between the various schools of constructivism.

Nevertheless, we find it convenient to take one particular approach as the general background (“framework”) for our discussion, viz. a (liberal) form of intuitionism. Consequently, this approach has been emphasized. The objective reasons for this choice are simple: most of the other constructive approaches can be described as restrictions or variants of this form of intuitionism (e.g. finitism as a restriction obtained by dropping “abstract” objects), but not vice versa. We are not concerned with the presentation of this framework as a closed whole, however.

1.3. Although “constructive” as used in this chapter does not refer to a clear-cut, sharply delimited part of mathematics, the various trends have something in common: they all satisfy the demands of “naive” constructivism, corresponding to a naive use of “constructive” which is commonplace among mathematicians (“naive” not used in a derogatory sense here). This naive use concerns the interpretation of existential statements: a proof of $\exists x Ax$ is constructive if we can find a particular x (term of our language), satisfying A , from the proof. Whatever the precise extent of constructivity, one is usually not in doubt as to this requirement (compare

this to the naive idea of *area of a surface* or *set*, ideas which are unproblematic in the case of a finite set and area of a rectangle). A typical example is the proof of the following

THEOREM. *There exist two irrational numbers a and b such a^b is rational.*

A non-constructive proof can be given as follows. $(\sqrt{2})^{\sqrt{2}}$ is either rational or irrational. In the first case, we may take $a = b = \sqrt{2}$; in the second case, we may take $a = (\sqrt{2})^{\sqrt{2}}$, $b = \sqrt{2}$, since then $a^b = 2$.

It would be easy to multiply such examples. The demands of naive constructivism often can be expressed quite well in mathematical terms which do not at all refer to “constructivity”: if $\exists x A(x, y_1, \dots, y_n)$ expresses the existence of a solution of a diophantine equation with parameters $y_1, \dots, y_n$, there is an obvious difference between a result which gives us a bound on the *number of solutions* for x , in terms of the parameters, and a result which gives us a bound on the (size of the) solutions themselves.

Already naive constructivism leads to interesting metamathematical problems; e.g. when we prove something of the form $\exists x ((Ax \wedge x = t_1) \vee (Ax \wedge x = t_2))$ for known terms t_1, t_2 , can we also prove $\exists x (Ax \wedge x = t_1)$ or $\exists x (Ax \wedge x = t_2)$? (Cf. the example.) A restriction on the logical rules turns out to be necessary; but which restriction? Is there a re-interpretation of the logical operators corresponding to this restriction? Such questions lead us rapidly out of the domain of naive constructivism.

1.4. Sometimes, the meaning of “constructive” is stretched even farther, and is taken to include views such as predicativism (e.g. WEYL [1918], or Gödel’s footnote (added for the reprinting) in BENACERRAF and PUTNAM [1964, p. 211]), where the underlying logic is classical, and where the restrictions concern only the definition principles admitted; but classical predicativism falls outside the scope of this chapter.

Another constructivistic trend where the underlying logic is classical, is *classical recursive analysis* RA; this will be occasionally discussed for comparison.

1.5. The principal aspects of constructivism we shall discuss are:

(i) The role of logic and abstract concepts (e.g. as “abbreviation”, making arguments more intelligible); reductions to quantifier-free statements; interpretation of the logical operations (see Sections 2, 5.7, 7.2, 11.4).

(ii) “Intensional” aspects. When interpreted in the widest sense, this is a

very common phenomenon, also in classical mathematics; but in constructive mathematics we often have to pay attention to the way an object is *given* to us, where classically this is not necessary. (Example: a real number is *given* to us as a real-number generator, i.e. a Cauchy sequence of rationals.) See for these aspects 4.2(ii), 10.3, 10.4, 11.7(iii).

(iii) The validity of Church's thesis (see Section 4).

(iv) Continuity axioms, the possibility of a theory of continuous quantification (Section 6).

(v) Usefulness of the subjectivistic interpretation (2.2(i), 7.2).

(vi) The quest for explicit definability (4.15).

(vii) Markov's schema (Section 8).

(viii) Connection between validity for intuitionistic predicate logic and mathematical assumptions (Section 9).

(ix) The existence of classical counterparts to problems of constructive mathematics (4.14, 5.14) and systematic procedures for constructivizing classical theorems (Section 12).

Of course, many of these aspects are interrelated: for example, Church's thesis very blatantly requires attention to intensional aspects, and a special form of Markov's schema enters in the discussion of (viii). For expository reasons, we have not divided the paper according to these aspects.

The concept of natural number, induction over the natural numbers, and the introduction of rationals and integers we regard as unproblematic and is taken for granted.

In drawing attention to various aspects of constructivism, we shall introduce various metamathematical methods which can be used for studying those aspects, such as realizability and elimination of choice sequences. This chapter is not a survey of constructivism, only a survey of aspects; nor do we claim completeness for the bibliography; the items in the bibliography are included either for historical reasons or to assist in further study of the subjects discussed.

How to read this chapter. For readers with little or no experience with constructive mathematics, the best order is probably to start with Section 1, then 2.1 and 2.2, Section 5, 6.1–6.4 (some notations used there are explained in 3.7); and then to return to the metamathematical developments: 2.3–2.5, Sections 3 and 4, 6.5–6.23, Sections 7–12.

For those readers who are more or less familiar with constructive mathematics, the chapter may be read in regular order, skipping Section 5 (except for consultation when needed later on).

Both categories of readers may skip Sections 7 and 9 on a first reading.

2. Logic

2.1. We first describe, as a starting point, the Brouwer–Heyting–Kreisel (“BHK” for short) explanation of the logical operations. We point out in advance that

(1) we do not aim at a detailed development of these explanations;
 (2) they are not intended to be “reductive”, i.e. to give an explanation in terms of *simpler* notions which are already understood (note that the classical truth-definition for logical operators is also not “reductive” in this sense);

(3) the principal purpose of these explanations is to serve as a point of reference to compare other interpretations with (e.g. realizability, 4.3). The explanation uses the primitive concept of (constructive) proof and construction, and tells us the meaning of “proof of a compound statement” in terms of “proof of a constituent”.

(a) A proof of $A \wedge B$ consists in a proof of A and a proof of B .

(b) A proof of $A \vee B$ consists in specifying a proof of A or a proof of B .

(c) A proof of $A \rightarrow B$ consists of a construction c which transforms any proof of A into a proof of B (*together* with the insight that c has the property: d proves $A \Rightarrow cd$ proves B).

(d) $\perp$ is an unprovable statement. Hence a proof of $\neg A$ (defined as $A \rightarrow \perp$) is a construction which transforms any proof of A into a proof of $\perp$.

(e) If the variable x ranges over a “basic” domain D (i.e. a domain where each construction (object) belonging to it is *given* as such; in other words, the elements d of D “carry their own proof” that they belong to D), we can explain a proof of $\forall x Ax$ as a construction c which on application to any $d \in D$ yields a proof $c(d)$ of Ad , together with the insight that c has this property. The natural numbers are an example of such a basic domain.

If D is an arbitrary domain, c should act on a pair d, d' , d an element of D , d' a proof that $d \in D$.

(f) For x ranging over a basic domain D , a proof of $\exists x Ax$ is given as a pair c, d , c a proof of Ad , $d \in D$.

For an arbitrary domain we need a triple (c, d, d') with c a proof of Ad , d' a proof of $d \in D$.

To illustrate this interpretation by an example, consider a statement of the form $C \equiv (A \rightarrow \exists x B)$; the proof of C contains a transformation τ of proofs of A into proofs of $\exists x Bx$, hence in particular τ shows how to obtain an x such that Bx from a proof of A . Classically, $(A \rightarrow \exists x B) \rightarrow$

$\exists x (A \rightarrow B)$ is justified; on the BHK-explanation, the x given by τ may depend essentially on (information contained in) a proof of A ; we cannot expect to determine the x *a priori*, as required for a proof of $\exists x (A \rightarrow Bx)$.

2.2. Remarks

2.2.1. It is plausible to assume “ c is a proof of A ” to be decidable, i.e. if a construction proves an assertion, one should be able to read off the assertion from the proof. (In subjectivistic terms: we recognize a proof when we see one; if we are in doubt, it is (to us) not a proof.)

2.2.2. This interpretation of the logical constants presents a first example of the introduction of *abstract* concepts in constructive mathematics (“proof”, “construction”); and it is our understanding of these concepts (reflection on them) which enables us to see that the laws of intuitionistic predicate logic are valid on this interpretation (whatever the *exact* extension of the concepts of proof and construction is, the explanation is sufficiently clear for this).

In finitism, one does not allow reflection on abstract concepts; one restricts oneself to considering “visualizable” objects. Thus one may consider natural numbers and *particular* rules representing number-theoretic functions; but the general (abstract) concept of a rule assigning to each natural number another natural number as value is not considered.

An assertion of the form $\forall x (t_1[x] = 0)$ (x ranging over natural numbers, t_1 a fixed term with parameter x) may be regarded as (finitistically) established if we have a method for establishing $t_1[\bar{n}] = 0$ for each numeral $\bar{n}$; $t_1[x] = 0 \rightarrow t_2[x] = 0$ is also unproblematic, because equivalent to $(1 \dot{-} t_1[x])t_2[x] = 0$, but

$$\forall x (t_1[x] = 0) \rightarrow \forall x (t_2[x] = 0) \quad (1)$$

cannot be “finitistically understood” as such; we can establish (1) in a finitistically meaningful way by describing a *particular* t such that

$$t_1[t[x]] = 0 \rightarrow t_2[x] = 0 \quad \text{for all } x. \quad (2)$$

2.2.3. On the BHK-explanation, a logically compound statement such as $\exists x Ax$ or $A \rightarrow B$ asserts the existence of certain information (i.e. a proof of such statements must contain that information) which is not made explicit in the statement. Replacing a logically compound mathematical statement by a corresponding one in which more of this information is made explicit may therefore be described as a move towards a more

“logic-free” formulation. A first example is the replacement of (1) by (2), in our discussion of finitism above.

Another example is the replacement of partially defined operations by total ones; for example suppose we have a statement involving a partial operation f :

$$\forall x (Ax \rightarrow !fx \wedge B(fx)). \quad (3)$$

($!fx$ stands for: fx is defined.) For any x and any proof of Ax we can construct fx . To show that fx is defined, and for its computation we need some information i contained in a proof of Ax ; to be definite, assume the possible i 's to be coded *onto* $\mathbb{N}$; making that information explicit, we can replace f by f' and Ax by $A'(i, x)$ ($\equiv$ “ Ax has a proof containing the information i ”) and reformulate (3) as

$$\forall i x (A'(i, x) \rightarrow B(f'(i, x))) \quad (4)$$

where f' is now total. Assuming $A'(i, x)$ to have a lower logical complexity than A , we have managed to replace (3) by a more “logic-free” statement. For a concrete example, see 5.7. Note however, that replacing logically compound statements by “logic-free” ones with more explicit information may result in a loss of intelligibility; from the viewpoint of constructive mathematics the problem is to add “enough, but not too much” additional information.

2.2.4. Unintended variants of the scheme of explanation given above are often more useful (in a technical sense) than the scheme itself: realizability is a case in point. The explanation given above is e.g. not accepted as basic by constructivists such as A.A. Markov and N.A. Šanin; we return to this matter in the discussion of realizability.

2.2.5. Implication is in character rather similar to universal quantification in this scheme of explanation; hence it is not surprising that the nesting of implications has to be counted for a suitable measure of logical complexity (in contrast to the classical case, where only the number of alternations of quantifiers has to be counted). The result of DE JONGH [1973, §5] illustrates this remark: there exists an A of $L[\mathbf{HA}]$ such that for no $B(x)$ of $L[\mathbf{HA}]$ $\mathbf{HA} \vdash B(\bar{n}) \leftrightarrow g_n(A)$ is provable for all n , where $g_n(P)$, $n = 0, 1, \dots$ enumerates all propositional formulae in one variable.

2.3. A formal system for intuitionistic predicate calculus (IPC)

Let us use x, y, z, u, v, w for individual variables, $t, t^1, \dots$ for terms, A, B, C for formulae, $\perp$ for absurdity. The various formalizations of intuitionistic predicate logic fall apart into three types:

(a) Hilbert-type systems (FITTING [1969]; KLEENE [1952]; TROELSTRA [1973a, 1.1.3]).

(b) Systems of natural deduction (PRAWITZ [1965]).

(c) Calculi of sequents (FITTING [1969]).

Each of these types has its own special uses, advantages and drawbacks. We describe here a Hilbert-type system which is quite convenient for metamathematical arguments by induction on the length of derivations, such as soundness proofs for interpretations. The system is taken from GÖDEL [1958]. As metamathematical operators we use

$$\Rightarrow, \Leftrightarrow$$

with the obvious interpretation.

- (1) $A, A \rightarrow B \Rightarrow B$;
- (2) $A \rightarrow B, B \rightarrow C \Rightarrow A \rightarrow C$;
- (3) $A \vee A \rightarrow A, A \rightarrow A \wedge A$;
- (4) $A \rightarrow A \vee B, A \wedge B \rightarrow A$;
- (5) $A \vee B \rightarrow B \vee A, A \wedge B \rightarrow B \wedge A$;
- (6) $A \rightarrow B \Rightarrow C \vee A \rightarrow C \vee B$;
- (7) $A \wedge B \rightarrow C \Rightarrow A \rightarrow (B \rightarrow C)$;
- (8) $A \rightarrow (B \rightarrow C) \Rightarrow A \wedge B \rightarrow C$;
- (9) $\perp \rightarrow A$;
- (10) $B \rightarrow Ax \Rightarrow B \rightarrow \forall x Ax$ (x not free in B);
- (11) $\forall x Ax \rightarrow At$ (t free for x in A);
- (12) $At \rightarrow \exists x Ax$ (t free for x in A);
- (13) $Ax \rightarrow B \Rightarrow \exists x Ax \rightarrow B$ (x not free in B).

In (10) and (13) the derivation of the premiss is not supposed to depend on assumptions containing x free.

2.4. The “unintended” interpretations of intuitionistic logic fall apart into two types:

(i) modifications of the scheme of the BHK-explanation: realizability and modified realizability, Dialectica interpretation (see 4.2 and 11.2);

(ii) “truth-value” type semantics, e.g. topological, Beth, and Kripke models.

The connection with the BHK-explanation is much more indirect in this

case. We shall not discuss this type of semantics in detail here. Some remarks are contained in Section 9.

The various truth-value type semantics show that the rules of intuitionistic logic crop up at various places in the disguise of well-known classical structures — and it is perhaps worth mentioning here that the “logic” of forcing is in fact intuitionistic logic (KRIPKE [1965], pp. 118–120).

It seems therefore that, quite independently of any philosophical bias, intuitionistic logic may claim a certain interest in its own right.

For the various types of interpretations (semantics) one can of course investigate the problem of completeness. For the various “truth-value” type semantics there exist at least classical completeness proofs — but on the other hand, with respect to the intuitive validity concept as “constructively true in all structures” we have only partial results. (See the remarks in Section 9; a survey of completeness for the intuitive validity concept is in TROELSTRA [1977b].)

2.5. Some formal properties of IPC; references

2.5.1. Various formal systems for **IPC**: natural deduction calculus in PRAWITZ [1965]; sequent calculi in PRAWITZ [1965], Appendix A; KLEENE [1952], Ch. XV; FITTING [1969], Ch. 5, §1; Ch. 6, §4; Hilbert-type calculi in TROELSTRA [1973a], 1.1.3, 1.1.4; FITTING [1969], Ch. 5, §7, 8; KLEENE [1952], Ch. IV. The references also contain equivalence proofs between various systems.

2.5.2. Already the monadic fragment (with one monadic predicate letter) of **IPC** is undecidable; for a proof, due to D.M. Gabbay, see e.g. SMORYNSKI [1973b], p. 115, III B. The class of prenex formulae is decidable: KLEENE [1952], §80 gives a decision method for propositional formulae which is readily extended to prenex formulae.

2.5.3. Cut elimination and normalization: PRAWITZ [1965], Ch. IV; KLEENE [1952], Ch. XIV.

2.5.4. **IPC** possesses DP and ED:

DP $\vdash A \vee B \Rightarrow \vdash A \text{ or } \vdash B,$

ED $\vdash \exists x Ax \Rightarrow \vdash At \text{ for a suitable term } t;$

this can be obtained as a consequence of 2.5.3. For a generalization of DP, ED, see KLEENE [1962, 1963].

2.5.5. The interpolation theorem was first proved in SCHÜTTE [1962]; other proofs are in PRAWITZ [1965], Ch. IV, §3; FITTING [1969], Ch. 6, §5; an extension to the language with equality and function symbols is in NAGASHIMA [1966]. This result may be obtained as a corollary of 2.5.3.

2.5.6. For the connection between **CPC** (= classical predicate logic) and **IPC** see 3.8–3.10; KLEENE [1952], §81; an extension of this is in MINC and OREVKOV [1963].

2.5.7. For a more detailed discussion of the BHK-explanation see TROELSTRA [1969], §2. For the origin of this explanation see e.g. BROUWER [1954]; HEYTING [1931, 1954, 1955]; KREISEL [1965]. For a rival interpretation see MARTIN-LÖF [1975].

3. Some languages, formal systems and notations; the Gödel negative translation

3.1. The language of first-order arithmetic $L_0 = L[\mathbf{HA}]$

The language contains numerical variables (x, y, z, u, v, w), constants 0 (zero), S (successor), a constant for each primitive recursive function, $=$ (equality); furthermore the logical operators $\wedge, \vee, \forall, \exists, \rightarrow$; $\perp$ is identified with $0 = S0$.

3.2. The formal system of intuitionistic first-order arithmetic **HA**

The system is based on first-order predicate logic, axioms for equality and successor as usual, defining axioms for all primitive recursive functions, the induction schema. The system is sometimes called Heyting's Arithmetic.

3.3. Language $L_1 = L[\mathbf{EL}]$ of elementary analysis

We extend $L[\mathbf{HA}]$ with variables (a, b, c, d) for unary number-theoretic functions, constants $\mathbf{Ap}$ (for application), Π (for primitive recursion) and λx (abstraction operator for explicit definition); the logical operators are now extended with function quantifiers.

3.4. Elementary analysis **EL**

The axioms and schemata of **HA** are extended to the language of **EL**, the abstraction operator satisfies

$$(\lambda x. t[x])t' = t[t']$$

and the recursor Π

$$\Pi\phi t 0 = t, \quad \Pi\phi t (Sx) = \phi(\Pi\phi tx, x).$$

Finally we add

$$\text{QF} - \text{AC}_{00} \quad \forall x \exists y A(x, y) \rightarrow \exists a \forall x A(x, ax) \quad (A \text{ quantifier-free}).$$

As a convention, we shall write $\mathbf{EL}^*$ instead of $\mathbf{EL}$ if we use greek lower case letters $\alpha, \beta, \gamma, \delta$ to denote function variables; these variables are supposed to be distinct from the variables denoted by a, b, c, d . It is obvious that $\mathbf{EL}$ is a conservative extension of $\mathbf{HA}$: we only have to interpret the function variables as ranging over all total recursive functions.

It is more interesting, and much more difficult to prove that $\mathbf{HA} + \text{AC}_{01}$ is conservative over $\mathbf{HA}$, where AC_{01} is the schema $\forall x \exists a A(x, a) \rightarrow \exists b \forall x A(x, (b)_x)$; here $(b)_x = \lambda y. bj(x, y)$, where j is a (primitive recursive) pairing function from $\mathbb{N} \times \mathbb{N}$ onto $\mathbb{N}$. The first proof of this fact is in GOODMAN [1968]; a new, quite different proof is in MINC [1975].

3.5. The language $L_2 = L[\mathbf{HAS}]$ of second-order arithmetic

We add variables X, Y, Z for species (sets) of natural numbers to the language of $\mathbf{HA}$; prime formulae are now of the form $t_1 = t_2$ or Xt_1 (alternatively $t_1 \in X$); set-quantifiers are also added.

3.6. Second-order arithmetic: $\mathbf{HAS}$

$\mathbf{HA}$ is now extended by addition of a comprehension schema

$$\text{CA} \quad \exists X \forall x [Ax \leftrightarrow Xx]$$

(A any formula of $L[\mathbf{HAS}]$ not containing X free).

3.7. Some notations and conventions

Most of our notations are standard. For reference below, we list here the principal ones.

3.7.1. Pairing, coding of finite sequences

j is supposed to be a primitive recursive pairing function mapping $\mathbb{N}^2$ onto $\mathbb{N}$, with primitive recursive inverses. We use as abbreviations

$$\phi(x, y) \equiv_{\text{def}} \phi j(x, y) \quad (\phi \text{ unary function}),$$

$$X(x, y) \equiv_{\text{def}} Xj(x, y) \quad (X \text{ set variable}).$$

We assume a primitive recursive coding of finite sequences of natural numbers onto the natural numbers to be given;

$$\langle x_0, \dots, x_u \rangle \text{ is the code of } x_0, \dots, x_u,$$

$$\langle \quad \rangle = 0,$$

$$\hat{x} \equiv_{\text{def}} \langle x \rangle.$$

lth indicates the length function, * concatenation, $(n)_x$ is a function satisfying for $n = \langle x_0, \dots, x_u \rangle$,

$$(n)_y = x_y \quad \text{for } y \leq u, \quad (n)_y = 0 \quad \text{for } y > u;$$

* and $\lambda n \lambda y. (n)_y$ are supposed to be primitive recursive.

3.7.2. Notations concerning functions

$$\bar{\alpha}x \equiv_{\text{def}} \langle \alpha 0, \dots, \alpha(x-1) \rangle, \quad \bar{\alpha}0 = \langle \quad \rangle;$$

$$n \leq m \equiv_{\text{def}} \exists n' (n * n' = m), \quad n < m \equiv_{\text{def}} n \leq m \wedge n \neq m;$$

$$\alpha \in n \equiv_{\text{def}} \exists x (\bar{\alpha}x = n);$$

$$\alpha(\beta) \simeq x \equiv_{\text{def}} \exists y (\alpha(\bar{\beta}y) = x + 1), \quad !\alpha(\beta) \equiv_{\text{def}} \exists !x (\alpha(\beta) \simeq x);$$

$$(\alpha \mid \beta)(x) \simeq y \equiv_{\text{def}} \exists z (\alpha(\hat{x} * \bar{\beta}z) = y + 1);$$

$$\alpha \mid \beta \simeq \gamma \equiv_{\text{def}} \forall x ((\alpha \mid \beta)(x) \simeq \gamma x);$$

$$!\alpha \mid \beta \equiv_{\text{def}} \exists !\gamma (\alpha \mid \beta \simeq \gamma);$$

$$\alpha \leq \beta \equiv_{\text{def}} \forall x (\alpha x \leq \beta x).$$

3.7.3. Notations of elementary recursion theory

Partial recursive function application is indicated by Kleene brackets $\{\cdot\}\cdot$; T denotes Kleene's T -predicate, U the result extracting function. So

$$\{x\}(y) \simeq z \leftrightarrow \exists u (T(x, y, u) \wedge Uu = z).$$

Let t be a term-expression including Kleene-brackets. Then

$$!t \equiv t \text{ is defined,} \quad !t \wedge At \equiv \exists x (t \simeq x \wedge Ax).$$

$\lambda x. t$ is a Gödel number of t as partial recursive function of x , primitive recursive in the other parameters.

3.7.4. Formal systems

Formal systems are indicated by boldface letters (**H**, **IPC**, **HA** etc.); $L[\mathbf{H}]$ is the language of **H**. Schemata are often denoted by combinations of

letters: CONT_0 , $\text{AC} - \text{NN}$, $\text{WC} - \text{N!}^*$, chosen in agreement with KREISEL and TROELSTRA [1970], TROELSTRA [1977a].

3.8. The negative translation: definition

For any of the languages considered (and the languages of finite types to be discussed later) we define a mapping ' inductively by

- (i) $P' \equiv \neg\neg P$ for P prime,
- (ii) $(A \wedge B)' \equiv A' \wedge B'$,
- (iii) $(A \rightarrow B)' \equiv A' \rightarrow B'$,
- (iv) $(\forall x A)' \equiv \forall x A'$,
- (v) $(A \vee B)' \equiv \neg(\neg A' \wedge \neg B')$,
- (vi) $(\exists x A)' \equiv \neg\forall x \neg A'$.

(Here x is any sort of variable occurring in the system under discussion.) We shall agree to simplify ' for the case of formal systems where the prime formulae are decidable by replacing (i) by: (i') $P \equiv P'$ for P prime.

3.9. DEFINITION. If A does not contain $\exists$, $\vee$ we call A $\exists$ -free. If A is $\exists$ -free and all prime-formulae in A occur negated, A is said to be *negative*. (For systems with decidable prime formulae negative and $\exists$ -free formulae coincide modulo logical equivalence.) The class of *Harrop-formulae* Δ is defined inductively by

- (i) doubly negated prime formulae belong to Δ ,
- (ii) $A, B \in \Delta \Rightarrow A \wedge B \in \Delta$,
- (iii) $A \in \Delta \rightarrow \forall x A \in \Delta$,
- (iv) $B \in \Delta \Rightarrow A \rightarrow B \in \Delta$.

(For systems with decidable prime formulae, the "doubly negated" in (i) may be omitted.) All negative formulae are equivalent to Harrop formulae.

LEMMA. For a formal system $\mathbf{H}$ based on many-sorted intuitionistic predicate logic, A a Harrop-formula, $\mathbf{H} \vdash A \leftrightarrow \neg\neg A$.

PROOF. By induction on the complexity of A , using repeatedly the logical laws $\neg\neg(A \wedge B) \leftrightarrow (\neg\neg A \wedge \neg\neg B)$, $A \rightarrow \neg\neg A$, $\neg\neg\forall x A \rightarrow \forall x \neg\neg A$, $\neg\neg(A \rightarrow B) \leftrightarrow (A \rightarrow \neg\neg B)$. $\square$

THEOREM. For $\mathbf{H} = \mathbf{HA}, \mathbf{HAS}, \mathbf{IPC}$,

$$\mathbf{H}^c \vdash A \Leftrightarrow \mathbf{H} \vdash A'.$$

PROOF. Straightforward by induction on the length of derivations, using the preceding lemma. $\square$

3.10. Historically, a translation of this type was first given in KOLMOGOROV [1925] (for logic). The better-known GÖDEL [1933] also treats arithmetic; the present variant is due to GENTZEN [1969]. See also KLEENE [1952], §81.

4. Realizability and Church's thesis

4.1. If one accepts the BHK-explanation of the logical operators and the natural numbers, the interpretation of **HA** poses no problems, but we have not yet committed ourselves as to the interpretation of the number-theoretic functions in **EL**.

One possible interpretation is: the function variables range over lawlike number-theoretic functions, i.e. functions which are completely given to us by a law, a "recipe" for computing a value for each argument. Church's thesis can now, in the language of **EL**, be expressed as "every lawlike function is recursive" or formally

$$\text{CT} \quad \forall a \exists x \forall y \exists z [T(x, y, z) \wedge ay = Uz].$$

From the viewpoint of the Russian constructivist school, this is even the only possible interpretation: in their mechanistic approach, "recursive" is accepted as the mechanically precise form of "lawlike". In the traditional intuitionistic approach, CT is *not* self-evident — there is a certain gap in the arguments which claim to show that mechanically computable = humanly computable (for an extensive discussion see KREISEL [1972]).

The interpretation of the logical constants suggests that in fact the following axiom of choice should hold: $(AC_{00} =)$

$$\text{AC} - \text{NN} \quad \forall x \exists y A(x, y) \rightarrow \exists a \forall x A(x, ax),$$

since a proof of the premiss of this implication must contain a method which produces for every x a y such that $A(x, y)$; and this method is nothing else but a lawlike function. As soon as we start restricting the lawlike functions, AC – NN is not obvious any more. AC – NN plus CT yields

$$\text{CT}_0 \quad \forall x \exists y A(x, y) \rightarrow \exists u \forall x \exists z [Tuxz \ \& \ A(x, Uz)]$$

which is also meaningful w.r.t. **HA**.

From an intuitionistic point of view CT_0 is problematic, i.e. it is not obviously true nor obviously consistent when added to **HA**. From the viewpoint of the Russian constructivist school (CRA) the problem is rather to give an interpretation of the logical operators in arithmetical statements which is in agreement with CT_0 .

4.2. Remarks

(i) In the BHK-explanation of logic, and the justification of AC – NN just given, we have examples of how certain abstractly formulated concepts are accepted and axioms justified by reflection on the abstract concepts. In this, the intuitionist approach goes beyond finitism (cf. 2.2.2), and also beyond CRA, where ranges of variables are supposed to be listable (i.e. effectively enumerable) or (via relativization of quantifiers) definable subsets of listable ranges — so AC – NN does not even make sense if we think of lawlike functions “in the abstract”.

(ii) CT forces us to pay attention to intensional aspects. For example, the justification of AC – NN just given might tempt us to defend a generalization

$$\forall x \in X \exists y \in Y A(x, y) \rightarrow \exists \Psi \in (X \rightarrow Y) \forall x \in X A(x, \Psi x).$$

If we applied this to CT, we would find

$$CT \rightarrow \exists \Psi \forall a \forall y \exists z [T(\Psi a, y, z) \ \& \ ay = Uz]$$

but, assuming CT to be true, elementary recursion theory tells us that there is no Ψ representable as a partial recursive operation on total recursive functions such that

$$\forall x (ax = bx) \rightarrow \Psi a = \Psi b$$

i.e. no Ψ which has functional character w.r.t. *extensional* equality. It is easy to see therefore why the generalization of the choice axiom fails w.r.t. extensional equality: the method giving a y to each $x \in X$ (an x to each a in the case of CT) can use much more than only the “extension” of x : in principle the method may use *all* available information on x (and notably, in the case of total recursive functions, their Gödel number).

We shall encounter many more examples where non-extensional information is relevant — in the example above, we can only speak of a functional Ψ if we admit non-extensional operations.

4.3. Realizability

Now we shall describe a re-interpretation of arithmetical formulas, originally devised by Kleene (KLEENE [1945]) to make the constructive interpretation of $\vee$ and $\exists$ more explicit, which will enable us to show consistency of CT_0 with **HA** and extensions of **HA**, and which has produced many interesting metamathematical results besides.

To each formula $A(x_1, \dots, x_n)$ of $L[\mathbf{HA}]$, containing at most $x_1, \dots, x_n$ free, we shall associate another formula of $\mathbf{HA}$, written as $x \mathbf{r} A(x_1, \dots, x_n)$ (“ x realizes A ”) containing at most $x, x_1, \dots, x_n$ free, $x \notin \{x_1, \dots, x_n\}$. The definition is by induction on the complexity of A .

- $\mathbf{r(i)} \quad x \mathbf{r} (t_1 = t_2) \equiv_{\text{def}} (t_1 = t_2),$
- $\mathbf{r(ii)} \quad x \mathbf{r} (A \wedge B) \equiv_{\text{def}} (j_1 x \mathbf{r} A \wedge j_2 x \mathbf{r} B),$
- $\mathbf{r(iii)} \quad x \mathbf{r} (A \vee B) \equiv_{\text{def}} [(j_1 x = 0) \rightarrow j_2 x \mathbf{r} A] \wedge (j_1 x \neq 0 \rightarrow j_2 x \mathbf{r} B),$
- $\mathbf{r(iv)} \quad x \mathbf{r} (A \rightarrow B) \equiv_{\text{def}} \forall y (y \mathbf{r} A \rightarrow !\{x\}(y) \wedge \{x\}(y) \mathbf{r} B),$
- $\mathbf{r(v)} \quad x \mathbf{r} (\exists y A y) \equiv_{\text{def}} j_2 x \mathbf{r} A(j_1 x),$
- $\mathbf{r(vi)} \quad x \mathbf{r} (\forall y A y) \equiv_{\text{def}} \forall y (!\{x\}(y) \wedge \{x\}(y) \mathbf{r} A y).$

Note that if a prime formula is realizable, it is realized by every number; also note

(a) $(x \mathbf{r} \neg A) \leftrightarrow \forall y (y \mathbf{r} A \rightarrow !\{x\}(y) \wedge \{x\}(y) \mathbf{r} (1 = 0)) \leftrightarrow \forall y \neg (y \mathbf{r} A).$
Hence $\forall x (x \mathbf{r} \neg A) \leftrightarrow \exists x (x \mathbf{r} \neg A)$. So a negation is realized by any number if it is realized at all.

$$(b) \quad x \mathbf{r} \neg \neg A \leftrightarrow \forall y \neg (y \mathbf{r} \neg A) \leftrightarrow \forall y \neg \forall z (\neg z \mathbf{r} A) \\ \leftrightarrow \neg \forall z (\neg z \mathbf{r} A) \leftrightarrow \neg \neg \exists z (z \mathbf{r} A).$$

(c) As may be seen by inspection of the clauses of the definition, realizability is similar in spirit to (may be viewed as a variant of) the BHK-explanation.

In some respects it is coarser: $\forall x (t[x] = 0)$ may have many different proofs, but all Gödel numbers of all total recursive functions realize such a purely universal statement when it is true. On the other hand, realizability enforces recursiveness.

4.4. DEFINITION. A formula of $L[\mathbf{HA}]$ is *almost negative* if it is constructed from prime formulae or formulae $\exists x (t = s)$ by means of $\forall, \rightarrow, \wedge$.

4.5. LEMMA. For any almost negative $A(a)$, a non-empty string of numerical variables containing all the variables free in A , there is a partial recursive Ψ_A such that in $\mathbf{HA}$,

- (i) $A(a) \rightarrow !\Psi_A(a) \wedge \Psi_A(a) \mathbf{r} A(a);$
- (ii) $\exists x (x \mathbf{r} A) \rightarrow A.$

PROOF. By simultaneous induction on the complexity of A , defining Ψ_A as follows:

$$\begin{aligned}
\Psi_{t=s} &\equiv \Lambda a. 0 & \Psi_{\exists x (t=s)} &\equiv \Lambda a. [j(\min_x [t=s], 0)]; \\
\Psi_{A \wedge B} &\equiv \Lambda a. j(\Psi_A(a), \Psi_B(a)), & \Psi_{A \rightarrow B} &\equiv \Lambda ax. \Psi_B(a); \\
\Psi_{\forall x A} &\equiv \Lambda ax. \Psi_A(a, x). \quad \square
\end{aligned}$$

4.6. LEMMA. *For all A , $x \Vdash A$ is (in $\mathbf{HA}$) provably equivalent to an almost negative formula.*

PROOF. By induction on the complexity of A ; for example, $x \Vdash A \rightarrow B$ can be rewritten as $\forall y (y \Vdash A \rightarrow \exists z Txyz \wedge \forall u (Txyu \rightarrow Uu \Vdash B))$; then we can apply the induction hypothesis for A, B . $\square$

4.7. LEMMA. *Let ECT_0 (extended Church's thesis) denote the following schema:*

$$\text{ECT}_0 \quad \forall x [Ax \rightarrow \exists y Bxy] \rightarrow \exists z \forall x [Ax \rightarrow \exists u (Tz xu \wedge B(x, Uu))].$$

(A almost negative). Then there is a numeral $\bar{n}$ such that for any instance F of ECT_0 in $\mathbf{HA} \vdash \bar{n} \Vdash F$.

PROOF. Let $t = \{\{u\}(x)\} \Psi_A(x)$, then we can take

$$\bar{n} = \Lambda u. j(\Lambda x. j_1 t, \Lambda xw. j(\min_v T(\Lambda x. j_1 t, x, v), j(0, j_2 t)));$$

the verification is straightforward. $\square$

4.8. CHARACTERIZATION THEOREM. *For sentences A :*

- (i) (*Soundness*) $\mathbf{HA} + \text{ECT}_0 \vdash A \Rightarrow \mathbf{HA} \vdash \bar{n} \Vdash A$ for some $\bar{n}$.
- (ii) $\mathbf{HA} + \text{ECT}_0 \vdash A \Leftrightarrow \exists x (x \Vdash A)$,
- (iii) $\mathbf{HA} + \text{ECT}_0 \vdash A \Leftrightarrow \mathbf{HA} \vdash \exists x (x \Vdash A)$.

PROOF. (i) By induction on the length of derivations in $\mathbf{HA}$, using Lemma 4.7. The induction step consists in showing realizability of the universal closure of the conclusion from the assumption of the realizability of the universal closure of the premisses.

(ii) By induction on the complexity of A , with Lemma 4.6.

(iii) Combination of (i) and (ii). $\square$

4.9. COROLLARY. *$\mathbf{HA} + \text{ECT}_0$ is consistent relative to $\mathbf{HA}$; in fact, since by Lemma 4.5 $\exists x (x \Vdash A) \Leftrightarrow A$ for almost negative A , $\mathbf{HA} + \text{ECT}_0$ is a conservative extension of $\mathbf{HA}$ w.r.t. almost negative formulae.*

4.10. Thus we have obtained also that $\mathbf{HA} + \mathbf{CT}_0$ is conservative with respect to negative formulae. This result can easily be extended to $\mathbf{HAS}$, simply by extending the realizability as follows: To each set variable X we assign a set variable X^* (it may be the identity), and we put

- $\mathbf{r(i)'} \quad x \mathbf{r} Xy \equiv_{\text{def}} X^*(x, y),$
 $\mathbf{r(vii)} \quad x \mathbf{r} \forall X A(X) \equiv_{\text{def}} \forall X^*(x \mathbf{r} A(X)),$
 $\mathbf{r(viii)} \quad x \mathbf{r} \exists X A(X) \equiv_{\text{def}} \exists X^*(x \mathbf{r} A(X)).$

Now we can easily show:

THEOREM. $\mathbf{HAS} + \mathbf{CT}_0 + \mathbf{UP}$ is conservative over $\mathbf{HAS}$ w.r.t. negative formulae; here $\mathbf{UP}$ (Uniformity Principle) is the schema

$$\mathbf{UP} \quad \forall X \exists x A(X, x) \rightarrow \exists x \forall X A(X, x).$$

(For comments on $\mathbf{UP}$ see TROELSTRA [1973b].)

4.11. LEMMA. For any instance F of Markov's schema

$$\mathbf{M} \quad \forall x [Ax \vee \neg Ax] \wedge \neg \neg \exists x Ax \rightarrow \exists x Ax$$

there is a numeral $\bar{n}$ such that

$$\mathbf{HA} + \mathbf{M} \vdash \bar{n} \mathbf{r} F.$$

PROOF. We first note that with $\mathbf{CT}_0$, $\mathbf{M}$ is equivalent to

$$\mathbf{M}_{\text{PR}} \quad \neg \neg \exists y (t(x, y) = 0) \rightarrow \exists y (t(x, y) = 0).$$

For if $\forall x [Ax \vee \neg Ax]$, then with $\mathbf{CT}_0$ there is a z such that

$$\forall x \exists y [Tzxy \wedge (Uy = 0 \rightarrow Ax) \wedge (Uy \neq 0 \rightarrow \neg Ax)]$$

and thus $\exists x Ax \leftrightarrow \exists x \exists y [Tzxy \wedge Uy = 0]$ which can be expressed as $\exists u (t(z, u) = 0)$, t primitive recursive. So, since $\mathbf{HA} + \mathbf{ECT}_0 \vdash A \leftrightarrow \mathbf{HA} \vdash \exists x (x \mathbf{r} A)$, it is sufficient to show the lemma for instances of $\mathbf{M}_{\text{PR}}$, which is straightforward. This enables us to extend the characterization theorem to $\mathbf{HA} + \mathbf{M}$. $\square$

4.12. THEOREM. $\mathbf{HA} + \mathbf{M} + \mathbf{ECT}_0 \vdash A \leftrightarrow \mathbf{HA} + \mathbf{M} \vdash \exists x (x \mathbf{r} A).$

PROOF. Immediate with 4.8 and 4.11. $\square$

4.13. From the viewpoint of the Russian constructivist school (CRA), as

represented by N.A. Šanin and A.A. Markov, realizability is not a semantics since it does not reduce the interpretation of compound statements to simple ones (i.e. statements whose interpretations are regarded as more immediately evident). For example, one objection (ŠANIN [1958]) is that even formulae whose interpretation should be immediate, are replaced by more complicated ones by Kleene's realizability interpretation.

However, as to the *mathematical* consequences, we may certainly regard $\mathbf{HA} + \mathbf{M} + \mathbf{ECT}_0$ as a codification of the mathematical practice of CRA (cf. DRAGALIN [1973]) in view of Kleene's proof that Šanin's interpretation is provably equivalent to realizability relative to $\mathbf{HA} + \mathbf{M}$ (KLEENE [1960]). Instead of $\mathbf{ECT}_0$ one sometimes finds (as e.g. in DRAGALIN [1973])

$$\mathbf{ECT}' \quad \forall x [\neg Ax \rightarrow \exists y Bxy] \rightarrow \exists z \forall x [\neg Ax \rightarrow !\{z\}(x) \wedge B(x, \{z\}(x))]$$

which however is easily seen to be equivalent to $\mathbf{ECT}_0$ relative to $\mathbf{HA} + \mathbf{M}$ (noting that almost negative formulae are equivalent to negative formulae by $\mathbf{M}_{\text{PR}}$ ($\mathbf{M}$ restricted to primitive recursive A) and for negative A , $A \leftrightarrow \neg \neg A$ by 3.9, lemma).

4.14. For classical recursive analysis (RA) a somewhat hybrid situation exists: with respect to particular assertions (without parameters) the excluded third is used, but a statement from classical mathematics of the form $\forall x [Ax \vee \neg Ax]$ is "recursivized" by requiring a decision method for A , recursive in x . In short, the counterpart in RA of a closed statement A is the assertion $\exists x (x \Vdash A)$, which may be established by classical means. RA may be regarded as one possible answer to the search for an analogue to "constructive" within *classical* mathematics: recursiveness in parameters. For another solution "continuity in parameters", see 5.14.

4.15. Extensions and variants of realizability; explicit definability

4.15.1. A survey of realizability techniques for arithmetic is to be found in TROELSTRA [1971]; more detail is given in TROELSTRA [1973a], Ch. III. For analysis there are similar methods available; see 6.23.

4.15.2. One of the technically most useful variants is $\mathbf{q}$ -realizability ($x \mathbf{q} A$) obtained by changing clauses (iii), (iv), (v) in 4.3 to

$$\mathbf{q}(\text{iii}) \quad x \mathbf{q} (A \vee B) \equiv_{\text{def}} [(j_1 x = 0 \rightarrow (j_2 x \mathbf{q} A) \wedge A) \wedge$$

$$(j_1 x \neq 0 \rightarrow (j_2 x \mathbf{q} B) \wedge B)],$$

$$\mathbf{q}(\text{iv}) \quad x \mathbf{q} (A \rightarrow B) \equiv_{\text{def}} \forall y (y \mathbf{q} A \wedge A \rightarrow !\{x\}(y) \wedge \{x\}(y) \mathbf{q} B),$$

$$\mathbf{q}(\vee) \quad x \mathbf{q}(\exists y A) \equiv_{\text{def}} (j_2 x) \mathbf{q} A(j_1 x) \wedge A(j_1 x)$$

and replacing $\mathbf{r}$ by $\mathbf{q}$ in the other clauses.

The soundness theorem (cf. 4.8(i)) is then provable for $\mathbf{q}$ -realizability and yields results such as DP, ED (cf. 2.5.4) for $\mathbf{HA}$, and

$$\begin{aligned} \text{ECR}_0 \quad \mathbf{HA} \vdash Ax \rightarrow \exists y B(x, y) &\Rightarrow \\ &\Rightarrow \mathbf{HA} \vdash \exists z \forall x [Ax \rightarrow !\{z\}(x) \wedge B(x, \{z\}(x))] \end{aligned}$$

(A almost negative). Friedman recently adapted $\mathbf{q}$ -realizability to $\mathbf{HAS}$. Kleene's " $\Gamma \mid C$ " is another method particularly suited for proving DP, ED and related properties; in FRIEDMAN [1973] this is extended to higher-order systems such as $\mathbf{HAS}$. For an exposition of the essentials of this method see TROELSTRA [1973a], 3.1.21–3.1.23.

4.15.3. From the viewpoint of naive constructivism, it seems a natural question to ask for the strongest possible subsystem of classical logic still preserving DP, ED, when added to the mathematical axioms of the usual systems. But there is no unique answer: $\mathbf{HA} + \mathbf{M}$ and $\mathbf{HA} + \mathbf{IP}$ both possess DP, ED, but $\mathbf{HA} + \mathbf{M} + \mathbf{IP} = \mathbf{HA}^c$, i.e. classical first-order arithmetic. (Here $\mathbf{IP}$ is the schema $(\neg A \rightarrow \exists x B) \rightarrow \exists x (\neg A \rightarrow B)$, x not free in A ; $\mathbf{M}$ is defined in 4.11.) See TROELSTRA [1973a].

To see that $\mathbf{HA} + \mathbf{M} + \mathbf{IP} = \mathbf{HA}^c$, one proves by induction on the logical complexity of A that $\mathbf{HA} + \mathbf{M} + \mathbf{IP} \vdash A \vee \neg A$. Assume $A \vee \neg A$, then

- (1) $\forall x (A \vee \neg A) \wedge \neg \neg \exists x A \rightarrow \exists x A$, hence $\neg \neg \exists x A \rightarrow \exists x A$ (induction hypothesis), and by $\mathbf{IP} \exists y (\neg \neg \exists x Ax \rightarrow Ay)$; by the induction hypothesis again $\neg \neg \neg \exists x Ax \vee \exists y Ay$, hence $\exists x A \vee \neg \exists x A$, and
- (2) $\forall x Ax \leftrightarrow \neg \exists x \neg Ax$, hence

$$\begin{aligned} \forall x Ax \vee \neg \forall x Ax &\leftrightarrow (\neg \exists x \neg Ax \vee \neg \neg \exists x \neg Ax) \\ &\leftrightarrow \neg \exists x \neg Ax \vee \exists x \neg Ax \end{aligned}$$

(induction hypothesis).

5. Some elementary mathematics

5.1. In this section we develop a tiny part of constructive mathematics, in order to be able to illustrate some of our issues by means of examples taken from mathematics. Although most definitions run parallel to well-known classical ones, many classically equivalent definitions are not constructively equivalent, hence we have to pay attention to the exact formulation. For a readable account of the "recursive" approach, see e.g. MARTIN-LÖF [1970].

5.2. The basic universe

The theory of integers and rationals is unproblematic. We shall develop the theory of real numbers and real-valued functions relative to a certain universe $\mathcal{U}$ of number-theoretic functions; $\mathcal{U}$ is assumed to satisfy the axioms for functions of $\mathbf{EL}^*$. The principal axiom in $\mathbf{EL}^*$ concerning functions is the quantifier-free axiom of choice $\mathbf{QF-AC}_{00}$, which in fact modulo the other axioms expresses closure under “recursive in”. It is not hard to see that our condition on $\mathcal{U}$ is in fact equivalent to the following three conditions taken together.

- (1) $\mathcal{R} \subset \mathcal{U}$ (the recursive functions are contained in $\mathcal{U}$),
- (2) $\mathcal{U}$ is closed under pairing,
- (3) $\mathcal{U}$ is closed under all continuous operations represented by neighbourhood functions in $\mathcal{U}$.

The class of neighbourhood functions K_0 (relative to $\mathcal{U}$) is defined by

$$K_0\alpha \equiv \forall\beta \exists x (\alpha(\bar{\beta}x) \neq 0) \wedge \forall nm (\alpha n \neq 0 \rightarrow \alpha n = \alpha(n * m))$$

and the functional $\Phi_\alpha \in \mathbf{N}^{\mathbf{N}} \rightarrow \mathbf{N}^{\mathbf{N}}$ represented by α satisfies

$$(\Phi_\alpha\beta)(x) = y \leftrightarrow \exists z (\alpha(\langle x \rangle * \bar{\beta}z) = y + 1).$$

5.3. The real numbers

We choose the method of introduction by fundamental sequences. Let $\langle r_n \rangle_n$ be a standard-enumeration (without repetitions) of the rationals (if $p/q = r_n$, we may assume p, q to be found primitive recursively in n).

DEFINITION. $\langle r_{\alpha n} \rangle_n$ is said to be a *real number generator relative to $\mathcal{U}$* ($\mathcal{U}$ -r.n.g) if there is a β (*modulus of convergence*) such that

$$\forall k \forall m (|r_{\alpha\beta k} - r_{\alpha(\beta k + m)}| < 2^{-k}). \quad (1)$$

This is of course equivalent to the existence of a β' such that

$$\forall k \forall m_1 m_2 (|r_{\alpha\beta'(k+m_1)} - r_{\alpha\beta'(k+m_2)}| < 2^{-k}) \quad (1')$$

(given β , we can find β' by putting $\beta'k = \beta(k+1)$ for all k). We shall in the sequel omit “relative to $\mathcal{U}$ ” since $\mathcal{U}$ is kept fixed.

DEFINITION. Two real number generators $\langle s_n \rangle_n, \langle t_n \rangle_n$ with moduli β, γ respectively are said to be equivalent (notation: $\langle s_n \rangle_n \sim \langle t_n \rangle_n$) if for $\delta n = \max(\beta n, \gamma n)$,

$$|s_{\delta n} - t_{\delta n}| \leq 2^{-n+1}.$$

As in the classical theory, one shows $\sim$ to be an equivalence relation. Now the next step would be to define the reals $\mathbb{R}(\mathcal{U})$ ($\mathbb{R}$ for short) as equivalence classes of r.n.g.'s relative to $\sim$.

However we have not discussed set-existence so far. It is not *essential* for our specific purposes here, since instead of using the equivalence classes we could simply express everything by means of predicates and functions respecting $\sim$ (i.e. $P(\langle t_n \rangle_n) \wedge \langle t_n \rangle_n \sim \langle s_n \rangle_n \rightarrow P(\langle s_n \rangle_n)$ etc.); this course is adopted by KLEENE and VESLEY [1965], and in CRA.

But it is convenient to be able to talk about sets, and therefore as a minimum comprehension principle we shall adopt, relative to any given language L for which the interpretation already has been provided (in our case $L[\mathbf{EL}^*]$ is the relevant example), the following comprehension principle (X a variable for sets of individuals)

$$\exists X \forall x_1 \cdots x_n [A(x_1, \dots, x_n) \leftrightarrow X(x_1, \dots, x_n)], \quad (2)$$

A a formula of L , $x_1, \dots, x_n$ variables of L (L is not supposed to contain set variables). On the basis of this principle, we can accept well-defined properties of elements over a given domain as sets or relations. (2) justifies the introduction of reals as equivalence classes (by a metamathematical argument it is in fact easy to show that (2) is conservative over $\mathbf{EL}^*$, cf. TROELSTRA [1973a], 1.9.8).

5.4. Operations on, and relations between real numbers

In the usual style we may define operations and relations on reals by defining the corresponding operations and relations for r.n.g.'s, afterwards showing them to be invariant w.r.t. $\sim$. So for example

$$\langle s_n \rangle_n + \langle t_n \rangle_n \equiv \langle s_n + t_n \rangle_n, \quad \langle s_n \rangle_n \cdot \langle t_n \rangle_n \equiv \langle s_n \cdot t_n \rangle_n,$$

$$|\langle s_n \rangle_n| \equiv \langle |s_n| \rangle_n$$

etc., and

$$\langle s_n \rangle_n < \langle t_n \rangle_n \equiv \exists k \exists n \forall m (t_{n+m} - s_{n+m} > 2^{-k}).$$

Then for example, for $x, y \in \mathbb{R}$,

$$x < y \equiv \exists \langle s_n \rangle_n \in x \exists \langle t_n \rangle_n \in y (\langle s_n \rangle_n < \langle t_n \rangle_n),$$

$$x > y \equiv y < x,$$

$$x \leq y \equiv \neg(x > y), \quad x \geq y \equiv y \leq x.$$

REMARK ON NOTATION. In most of the intuitionistic literature, one writes $x \not\leq y$ for $x \leq y$, to avoid the suggestion that $x \leq y$ is equivalent to $x < y \vee$

$x = y$ (the latter assertion is much stronger). However, since our $\leq$ plays the same mathematical role as $\leq$ in classical mathematics, and since " $x < y \vee x = y$ " has no practical importance as a relation between reals, and moreover $\leq$ is easier to read than $\nless$, we have preferred here $\leq$ over $\nless$.

5.5. LEMMA (some properties of $+$, $\cdot$, $<$, $\leq$).

$$\begin{aligned} x \leq y \wedge y \leq x &\rightarrow x = y, \\ x \leq y \wedge y \leq z &\rightarrow x \leq z, \\ (x \leq y \wedge y < z) \vee (x < y \wedge y \leq z) &\rightarrow x < z, \\ x < y &\leftrightarrow x + z < y + z, \quad z > 0 \wedge x < y \rightarrow x \cdot z < y \cdot z, \\ x \leq y &\leftrightarrow \forall k (x < y + 2^{-k}); \quad \neg \neg x \leq y \leftrightarrow x \leq y. \end{aligned}$$

The proof is left to the reader; see e.g. HEYTING [1956], Ch. II.

5.6. Apartness and inequality between reals

Classically, the relations $\neq$ and $\#$ defined by (assuming $\langle s_n \rangle_n \in x$, $\langle t_n \rangle_n \in y$)

$$\begin{aligned} x \neq y &\equiv_{\text{def}} \neg \langle s_n \rangle_n \sim \langle t_n \rangle_n, \\ x \# y &\equiv_{\text{def}} \exists k \exists m \forall n (|s_{n+m} - t_{n+m}| > 2^{-k}) \end{aligned}$$

are equivalent. Relative to intuitionistic logic however, $x \neq y \leftrightarrow x \# y$ is equivalent to Markov's schema (see 8.2). For mathematical practice, the "positive" relation $\#$ is more important; the more so since $\neq$ can be defined in terms of $\#$, not vice versa.

Quite generally, a relation $\#$ satisfying

$$\begin{aligned} \text{S1} \quad & \neg x \# y \leftrightarrow x = y, \\ \text{S2} \quad & x \# y \rightarrow y \# x, \\ \text{S3} \quad & x \# y \rightarrow x \# z \vee z \# y, \end{aligned}$$

is called an *apartness relation*. Our relation $\#$ not only satisfies S1–S3, but in addition,

$$\begin{aligned} x \# y &\rightarrow x + z \# y + z, \quad x \# 0 \wedge y \# z \rightarrow xy \# xz, \\ x \# y &\leftrightarrow x < y \vee y < x. \end{aligned}$$

5.7. Partially defined operations

In inversion (i.e. the operation $x \mapsto x^{-1}$ for reals) we meet an example of a mapping which is not always defined, at least not in the natural sense (and, as will become clear in the sequel, *cannot* be defined constructively). With classical logic we easily remove this defect by an arbitrary convention, e.g. putting $0^{-1} = 0$, $(p/q)^{-1} = (q/p)$ for $p, q \neq 0$, and then defining

$$\begin{aligned} (\langle s_n \rangle_n)^{-1} &= \langle s_n^{-1} \rangle_n \quad \text{if } \langle s_n \rangle_n \notin 0 \\ &= \langle 0 \rangle_n \quad \text{otherwise.} \end{aligned}$$

Then, classically, $\langle s_n \rangle_n^{-1}$ is again an r.n.g. We cannot adopt this method in constructive mathematics, since we cannot assert $\forall x \in \mathbb{R} (x = 0 \vee x \neq 0)$.

Note that if we think of the reals in $\mathbb{R}^+ = \{x : x \in \mathbb{R} \wedge x \neq 0\}$ as *given* to us as r.n.g.'s $\langle s_n \rangle_n \in x$ together with a proof that $\langle s_n \rangle_n \neq 0$ (which implies that we have a k such that $|x| > 2^{-k}$), we see that we can avoid introducing x^{-1} as a partial operation by considering pairs (x, k) with the operation

$$(x, k) \mapsto (\max(2^{-k}, x))^{-1}.$$

Here we have a concrete example of replacing statements by more “logic-free” statements (see 2.2.3).

5.8. Weak counterexamples and their recursive counterparts

Traditional intuitionistic literature contains so called “weak counterexamples” to many mathematical assertions (such as: for all $x \in \mathbb{R}$, $x = 0 \vee x \neq 0$). These counterexamples are called “weak” because they do not refute the assertions involved, but show that the assumption of the existence of an intuitionistic proof for such assertions would lead to the solution of an as yet unsolved mathematical problem.

For example, let Ax be a decidable predicate of natural numbers (i.e. $\forall x (Ax \vee \neg Ax)$) such that $\neg \exists x Ax \vee \neg \neg \exists x Ax$ is unknown; a standard example of such a predicate is: “ x the number of the first decimal of the first sequence 0123456789 in the decimal fraction of π ”. Instead of A itself we can also use its characteristic function α

$$Ax \leftrightarrow \alpha x \neq 0.$$

Now define a real x_α depending on α via an r.n.g. $\langle s_n \rangle_n \in x_\alpha$ by

$$\begin{cases} \neg \exists y \leq x (\alpha y \neq 0) \rightarrow s_x = 0, \\ \alpha y \neq 0 \wedge y \leq x \wedge \forall z < y (\alpha z = 0) \rightarrow s_x = 2^{-y}. \end{cases} \quad (1)$$

It is easily verified that $\langle s_n \rangle_n$ is an r.n.g. and also that

$$\neg \exists y (\alpha y \neq 0) \leftrightarrow x_\alpha = 0, \quad \exists y (\alpha y \neq 0) \leftrightarrow x_\alpha \neq 0,$$

so $x_\alpha = 0 \vee x_\alpha \neq 0$ is equivalent to $\neg \exists y (\alpha y = 0) \vee \neg \neg \exists y (\alpha y = 0)$, and $x_\alpha = 0 \vee x_\alpha \neq 0$ to $\neg \exists y (\alpha y = 0) \vee \exists y (\alpha y = 0)$. This shows we have no grounds to assert $\forall x (x = 0 \vee x \neq 0)$, since this would require a solution to $\neg \exists x Ax \vee \neg \neg \exists x Ax$; and if this particular problem would be solved, we could obtain a new weak counterexample starting from another unsolved problem of the same type.

There is a connection with recursively unsolvable problems: the construction of the preceding counterexample depended on the existence of an α such that $\exists y (\alpha y = 0) \vee \neg \exists y (\alpha y = 0)$ was unknown. If we consider an α with an extra parameter z this becomes

$$\exists y (\alpha(y, z) = 0) \vee \neg \exists y (\alpha(y, z) = 0).$$

With $(\alpha)_z = \lambda z. \alpha(y, z)$ it follows that $\forall x \in \mathbb{R} (x = 0 \vee x \neq 0)$ implies

$$\forall z (x_{(\alpha)_z} = 0 \vee x_{(\alpha)_z} \neq 0)$$

hence

$$\exists y (\alpha(y, z) = 0) \vee \neg \exists y (\alpha(y, z) = 0) \quad \text{for all } z. \quad (2)$$

Now let $\{z : \exists y \alpha(y, z)\}$ represent an r.e. set which is not recursive; then the disjunction in (2) is not *recursively decidable* in z . As a result, we see that for the recursive reals $\mathbb{R}(\mathcal{R})$ $x = 0 \vee x \neq 0$ cannot be decided recursively in a parameter (and inversion cannot be defined on $\mathbb{R}(\mathcal{R})$ by a recursive operation).

Another type of weak counterexample, of which we shall encounter various examples below, depends on the existence of a problem of the following type: $\forall x (Ax \vee \neg Ax)$, $\forall x (Bx \vee \neg Bx)$, $\neg (\exists x Ax \wedge \exists x Bx)$, but $\neg \exists x Ax \vee \neg \exists x Bx$ is unknown. In terms of functions this becomes

$$\begin{cases} \neg (\exists y (\alpha y = 0) \wedge \exists y (\beta y = 0)) \text{ holds, while} \\ \neg \exists y (\alpha y = 0) \vee \neg \exists y (\beta y = 0) \text{ is unknown} \end{cases} \quad (3)$$

(an instance of such a problem is e.g. $Ax \equiv$ “ $2x$ is the number of the first decimal of the first sequence 0123456789 in the decimal expansion of π ” and $Bx \equiv$ “ $2x + 1$ is the number of the first decimal of the first sequence 0123456789 in the decimal expansion of π ”).

(3) can be used to give an example of a real (say x_0) such that $x_0 \leq 0 \vee x_0 \geq 0$ (hence a fortiori $x_0 < 0 \vee x_0 = 0 \vee x_0 > 0$) is unknown; define x_0 via a real number generator $\langle s_n \rangle_n \in x_0$ such that

$$\begin{cases} \neg(\exists y \leq n)(\alpha y = 0 \vee \beta y = 0) \rightarrow s_n = 0, \\ \alpha m = 0 \wedge \forall y < m (\alpha m \neq 0) \wedge m \leq n \rightarrow s_n = 2^{-m}, \\ \beta m = 0 \wedge \forall y < m (\beta m \neq 0) \wedge m \leq n \rightarrow s_n = -2^{-m}. \end{cases} \quad (4)$$

It is easy to verify that $\langle s_n \rangle_n$ is an r.n.g., and that for $\langle s_n \rangle_n \in x_0$ $x_0 \leq 0 \leftrightarrow \neg \exists y (\alpha y = 0)$, $x_0 \geq 0 \leftrightarrow \neg \exists y (\beta y = 0)$.

A recursive version of this counterexample depends on the existence of two disjoint r.e. sets which are not recursively separable: if $\{z: \exists y (\alpha(y, z) = 0)\}$, $\{z: \exists y (\beta(y, z) = 0)\}$ are such sets, then

$$\forall z \neg \{\exists y (\alpha(y, z) = 0) \mid \wedge \exists y (\beta(y, z) = 0)\} \quad (5.a)$$

while

$$\neg \exists y (\alpha(y, z) = 0) \vee \neg \exists y (\beta(y, z) = 0) \quad (5.b)$$

is not *recursively decidable* in z ; or, what amounts to the same, there is no *recursive* γ such that

$$\forall z \{(\gamma z = 0 \rightarrow \neg \exists y (\alpha(y, z) = 0)) \wedge (\gamma z \neq 0 \rightarrow \neg \exists y (\beta(y, z) = 0))\}. \quad (5.c)$$

For recursive reals this implies that $x \leq 0 \vee x \geq 0$ cannot be decided recursively in numerical parameters.

Another instructive example is discussed in the next subsection.

5.9. The representation of reals by binary expansions

Let $\mathbb{R}_2$ denote the class of reals permitting a binary expansion

$$\pm m + \left(\sum_{n=0}^{\infty} (\alpha n) 2^{-(n+1)} \right), \quad \alpha n \leq 1 \quad \text{for all } n.$$

Obviously $\mathbb{R}_2 \subseteq \mathbb{R}$, since $\langle \pm m + \sum_{k=0}^n (\alpha k) 2^{-(k+1)} \rangle_n$ is an r.n.g. Using *classical logic*, we can also show $\mathbb{R} \subseteq \mathbb{R}_2$ (i.e. for each r.n.g. we can find an equivalent binary expansion). To see this, argue as follows: an element x of $\mathbb{R}$ is either representable as

$$\pm m + \sum_{k=0}^n (\alpha k) 2^{-(k+1)}, \quad \alpha k \leq 1 \quad \text{for } 0 \leq k \leq n,$$

or not (i.e. x is either a “dyadic rational” or not). In the first case, we are done. In the second case, assume for simplicity $x \in [0, 1]$, and let $\langle s_n \rangle_n$ be an r.n.g. for x such that $|x - s_n| < 2^{-n}$ for all n , and assume

$$t_n = \sum_{k=0}^n (\alpha k) 2^{-(k+1)}$$

to be constructed such that

$$t_n < x < t_n + 2^{-(n+1)}$$

($t_n = x$ is excluded). Then since $x \neq t_n + 2^{-(n+2)}$, $(x < t_n + 2^{-(n+2)}) \vee (t_n + 2^{-(n+2)} < x)$; in the first case we put $\alpha(n+1) = 0$, in the second case $\alpha(n+1) = 1$, and define t_{n+1} accordingly.

On the other hand, if we consider $\frac{1}{2} + x_0$ (x_0 defined via an r.n.g. $\langle s_n \rangle_n$ as in (4) of the preceding section) and we assume $\frac{1}{2} + x_0$ to have a binary expansion $\sum_{n=0}^{\infty} (\alpha_n) 2^{-(n+1)}$, then $\alpha_0 = 0 \leftrightarrow \frac{1}{2} + x_0 \leq \frac{1}{2}$, $\alpha_0 = 1 \leftrightarrow \frac{1}{2} + x_0 \geq \frac{1}{2}$, which we cannot decide; and this weak counterexample is easily transformed into a proof of the fact that we cannot find the binary expansions for recursive elements of $\mathbb{R}$ by operations recursive in numerical parameters.

Similarly, we can show by *classical* reasoning that $\mathbb{R}_2$ is closed under $+$, $\cdot$, but on the recursive elements of $\mathbb{R}_2$ this cannot be done by a recursive mapping (cf. MAYOH [1965]).

5.10–5.12. Completeness of $\mathbb{R}$

5.10. DEFINITION. (i) A *sequence of reals* is given by a double sequence of r.n.g.'s $\langle \langle s_{m,n} \rangle_n \rangle_m$, and a function α such that, for each m , λn . $\alpha(m, n)$ is a modulus for $\langle s_{m,n} \rangle_n$.

A sequence $\langle x_m \rangle_m$ of reals is said to be a Cauchy-sequence if there is a modulus β such that

$$\forall k \forall m (|x_{\beta k} - x_{\beta(k+m)}| < 2^{-k}).$$

(ii) A sequence $\langle x_n \rangle_n$ has limit x (notation $\lim_n x_n$ or $\lim \langle x_n \rangle_n = x$), if there is an α (*limit-modulus*) such that

$$\forall k \forall m (|x - x_{\alpha k + m}| < 2^{-k}).$$

5.11. THEOREM. $\mathbb{R}(\mathcal{U})$ is complete, i.e. every Cauchy-sequence $\langle x_n \rangle_n$ has a limit.

PROOF. Let $\langle x_n \rangle_n$ be a Cauchy-sequence, $x_n = \langle s_{n,m} \rangle_m$, for each n , λm . $\alpha(n, m)$ is a modulus for $\langle s_{n,m} \rangle_m$; β is a modulus for $\langle x_n \rangle_n$. Therefore,

$$\forall k \forall n \forall m (|s_{n, \alpha(n, k)} - s_{n, \alpha(n, k) + m}| < 2^{-k}),$$

$$\forall k \forall n (|x_{\beta k} - x_{\beta k + m}| < 2^{-k})$$

and therefore, as is easily verified, $\langle s_{\beta n, \alpha(\beta n, \beta n + 1)} \rangle_n$ is an r.n.g.; let x be the corresponding real number. It is easy to see $\langle x_n \rangle_n$ converges to x with modulus function λn . $\beta(n+1)$. $\square$

5.12. REMARK. Note that the definitions of r.n.g., $\sim$, sequence of reals, Cauchy-sequence, sequence of reals converging to a limit become equivalent to their more usual definitions such as

$$\forall k \exists n \forall m (|s_n - s_{n+m}| < 2^{-k}),$$

$$\forall k \exists n \forall m (|s_{n+m} - t_{n+m}| < 2^{-k}),$$

$$\forall k \exists n \forall m (|x - x_{n+m}| < 2^{-k}),$$

for $\langle s_n \rangle_n$ r.n.g., $\langle s_n \rangle_n \sim \langle t_n \rangle_n$, $\lim_n x_n = x$ respectively, on assumption of the axiom of choice

$$\text{AC} - \text{NF} \quad \forall x \exists \alpha A(x, \alpha) \rightarrow \exists \beta \forall x A(x, (\beta)_x).$$

Since AC – NF is implied by ECT₀, we can in constructive recursive analysis (“the Russian school”) safely assume the usual definitions, just as in intuitionistic analysis developed in one of the usual theories of choice sequences.

For classical recursive analysis ((partial) functions from $\mathbb{N}$ into $\mathbb{N}$ are everywhere assumed to be (partial) recursive, but the logic is classical) this is not possible, since it is possible to define r.n.g.’s $\langle r_{\alpha n} \rangle_n$ with α not recursive by means of classical logic.

5.13. Real-valued functions

A real-valued function is a mapping $\mathbb{R} \rightarrow \mathbb{R}$. A real-valued function is said to be *continuous* if there is an operation $\Phi : \mathbb{R} \times \mathbb{N} \rightarrow \mathbb{N}$ such that

$$\forall k \forall x \in \mathbb{R} \forall y \in \mathbb{R} (|x - y| < 2^{-\Phi(x, k)} \rightarrow |fx - fy| < 2^{-k}).$$

A real-valued function is said to be *uniformly continuous* if there is a function $\alpha : \mathbb{N} \rightarrow \mathbb{N}$ such that

$$\forall k \forall x \in \mathbb{R} \forall y \in \mathbb{R} (|x - y| < 2^{-\alpha k} \rightarrow |fx - fy| < 2^{-k}).$$

Note that on assumption of AC₀₀ (or AC – NN), this is equivalent to the more customary formulation

$$\forall k \exists n \forall x \in \mathbb{R} \forall y \in \mathbb{R} (|x - y| < 2^{-n} \rightarrow |fx - fy| < 2^{-k}).$$

We define for $x, y \in \mathbb{R}$, $x \leq y$

$$(x, y) = \{z : x < z < y\}, \quad [x, y] = \{z : x \leq z \leq y\}.$$

Functions continuous or uniformly continuous on (x, y) or $[x, y]$ are defined similarly.

5.14. The existence of an l.u.b. and the intermediate-value theorem

We present two counterexamples to well-known theorems from classical analysis, showing at the same time how they have parallels in classical problems regarding solutions which are continuous in parameters.

5.14.1. EXAMPLE. Every uniformly continuous real-valued function f on $[0, 1]$ has a least upper bound $= \sup\{fx: x \in [0, 1]\}$, but we cannot expect to find effectively an $x_1 \in [0, 1]$ such that $f(x_1) = \sup\{f(y): y \in [0, 1]\}$. The positive statement about the existence of the l.u.b. is easily proved by considering

$$x_n = \sup\{f(k \cdot 2^{-n}): 0 \leq k \leq 2^n\}$$

and proving $\langle x_n \rangle_n$ to be a Cauchy-sequence of reals, which must have a limit in virtue of the completeness of $\mathbb{R}(\mathcal{U})$.

A weak counterexample is given by defining as in 5.8(4) an x_0 such that $x_0 > 0$, $x_0 = 0$, or $x_0 < 0$ is unknown.

Let $f(x) = x_0x + 1$. Assume now we could compute an x_1 s.t. $f(x_1) = \sup\{f(y): y \in [0, 1]\}$; then $x_1 < \frac{3}{4} \vee x_1 > \frac{1}{4}$.

If $x_0 > 0$, $x_1 = 1$, so $\neg x_1 < \frac{3}{4}$; if $x_0 < 0$, $x_1 = 0$, hence $\neg x_1 > \frac{1}{4}$. But $x_1 < \frac{3}{4} \vee x_1 > \frac{1}{4}$ requires $\neg x_0 > 0 \vee \neg x_0 < 0$, which we do not know. Transformation into an example showing the non-existence of a solution recursive in parameters is now routine (cf. 5.8 and 5.9).

In terms of classical mathematics we can express the content of the counterexample as follows. Small changes in f (in the sense of the uniform-continuity topology) result in big changes in the required x ; so we can state classically: for uniformly continuous f on $[0, 1]$, we cannot find an x_1 uniformly in f such that $f(x_1) = \sup\{f(y): y \in [0, 1]\}$.

5.14.2. EXAMPLE (see Fig. 1). Let f be uniformly continuous on $[0, 1]$. $f(0) < 0$, $f(1) > 0$. By a weak counterexample we can show that we cannot find an x such that $f(x) = 0$. For our counterexample we take the uniformly continuous f satisfying (x_0 as before)

$$x \in [0, 3^{-1} + 3^{-1}x_0] \rightarrow f(x) = 3x - 1,$$

$$x \in [3^{-1} + 3^{-1}x_0, 2 \cdot 3^{-1} + 3^{-1}x_0] \rightarrow f(x) = x_0,$$

$$x \in [2 \cdot 3^{-1} + 3^{-1} \cdot x_0, 1] \rightarrow f(x) = 3x - 2.$$

Clearly, if $x_0 < 0$, $f(x) = 0 \rightarrow x = 2 \cdot 3^{-1}$ and if $x_0 > 0$, $f(x) = 0 \rightarrow x = 3^{-1}$. Now if $f(x_1) = 0$, $x_1 < 3^{-1} \vee x_1 > 2 \cdot 3^{-1}$, hence $\neg(x_0 < 0) \vee \neg(x_0 > 0)$ which we do not know.

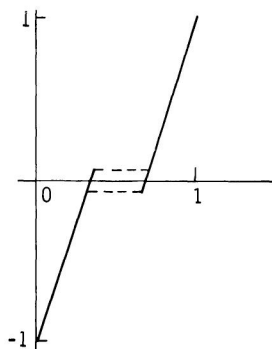


Fig. 1.

Classically, the result has its counterpart in the statement that the solution of $f(x_1) = 0$ cannot be found continuously in f . Note on the one hand that by classical logic, for a recursive f there is always a recursive x such that $f(x) = 0$ (by a reasoning quite similar to the argument showing that $\mathbb{R} \subseteq \mathbb{R}_2$ (5.9)). On the other hand, the standard transformation to a recursive version of this counterexample shows that there is no solution recursive in f , hence a fortiori not a recursively continuous one.

Remark. Similarly, we may construct a counterexample to Brouwer's fixed point theorem in one dimension: let f be a uniformly continuous function on $[0, 1]$ determined by: $x \in [2 \cdot 3^{-1} - x_0, 1] \rightarrow fx = 2 \cdot 3^{-1}$, $x \in [3^{-1} - x_0, 2 \cdot 3^{-1} - x_0] \rightarrow fx = x + x_0$, $x \in [0, 3^{-1} - x_0] \rightarrow fx = 3^{-1}$. f maps $[0, 1]$ on to $[3^{-1}, 2 \cdot 3^{-1}]$, but we cannot find an x such that $fx = x$. This example can be made into a two-dimensional counterexample in a trivial way: $g : (x, y) \mapsto (fx, 2^{-1}y + 2^{-2})$, defined on $[0, 1] \times [0, 1] = I^2$.

Classically, the recursive version of *this* counterexample to Brouwer's theorem only shows that the fixed point cannot be found recursively in f , but in fact in the two-dimensional case *much stronger* counterexamples can be given (OREVKOV [1963, 1964]) showing that (a) there exists a continuous mapping ϕ of the square I^2 into I^2 such that $\rho(p, \phi p) \geq 1/8$ for all $p \in I^2$, ρ an Euclidean metric, and (b) there exists a uniformly continuous mapping ψ from I^2 into I^2 such that $\forall p \in I^2 (\psi p \neq p)$.

5.15. Metric spaces

5.15. DEFINITION. (i) A *metric space* is a pair $\langle V, \rho \rangle$, where V is a set (the set of points of the space), and ρ a mapping $V \times V \rightarrow \mathbb{R}(\mathcal{U})$, such that

- (1) $\rho(x, y) \geq 0$, $\rho(x, y) = 0 \leftrightarrow x = y$,
- (2) $\rho(x, y) = \rho(y, x)$,
- (3) $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$.

(ii) A *complete separable metric* space is constructed as follows. Let a countable sequence of objects $\langle p_n \rangle_n$ with metric ρ be given, say by a β such that

$$|\rho(p_i, p_j) - r_{\beta(i, j, k)}| < 2^{-k}.$$

We now define *point-generators* (p.g.) similar to r.n.g.'s, ρ replacing $\lambda xy |x - y|$ in the definition; *equivalence* $(\langle p_{\alpha n} \rangle_n \sim \langle p_{\beta n} \rangle_n)$ is also defined as for r.n.g.'s. *Points* are now equivalence classes of p.g.'s; and ρ is automatically extended to all points by defining, if $\langle p_{\alpha n} \rangle_n \in x$, $\langle p_{\beta n} \rangle_n \in y$, $\langle p_{\alpha n} \rangle_n, \langle p_{\beta n} \rangle_n$ p.g.'s,

$$\rho(x, y) \equiv_{\text{def}} \lim_n \rho(p_{\alpha n}, p_{\beta n}).$$

Each p_n is embedded in the space as the equivalence class of $\langle p_n \rangle_n$, and ρ is simply an extension of the ρ on $\langle p_n \rangle_n$ modulo this embedding. An arbitrary *separable metric space* is a subspace of a complete separable metric space.

5.16. Standard representation of a complete separable metric space

Let $\lambda i. \alpha(k, n, i)$ enumerate the set

$$A_{n, k} \equiv_{\text{def}} \{i: \rho(p_i, p_n) < 2^{-k}\}.$$

$A_{n, k}$ is easily seen to be enumerable, since

$$A_{n, k} = \{i: \exists l (r_{\beta(i, n, l)} < 2^{-k} - 2^{-l})\}.$$

(If $\rho(p_i, p_n) < 2^{-k}$, also $\rho(p_i, p_n) < 2^{-k} - 2^{-l+1}$ for some l , hence $r_{\beta(i, n, l)} < \rho(p_i, p_n) + 2^{-l} < 2^{-k} - 2^{-l}$; and if $r_{\beta(i, n, l)} < 2^{-k} - 2^{-l}$, then also $\rho(p_i, p_n) < 2^{-k}$.)

Now we can associate to any $\gamma \in \mathcal{U}$ a sequence $\langle q_n \rangle_n$ of points from $\langle p_n \rangle_n$ such that

(1) $q_n = p_{\delta n}$, where $\delta 0 = \gamma 0$, and $\delta(n+1) = \alpha(n, \delta n, \gamma n)$.

It is easy to see that

(2) $\lim_n q_n = x \rightarrow \forall m (\rho(q_n, x) < 2^{-n+1})$, and each $\langle q_n \rangle_n$ defined as in (1) has a limit.

Let us denote the $x = \lim_n q_n$ for $\langle q_n \rangle_n$ obtained from γ as in (1) by x_γ .

(3) $\forall x \exists \gamma (x = x_\gamma)$.

(4) Let $V_{\tilde{\gamma}n} = \{x_\epsilon: \bar{\epsilon}n = \tilde{\gamma}n\}$, then

$$\forall x \exists \gamma (x = x_\gamma \wedge \forall k (U(2^{-k-2}, x) \subset V_{\tilde{\gamma}k})),$$

where $U(\epsilon, x) = \{y: \rho(x, y) < \epsilon\}$. To see this, take x, y such that $\rho(x, y) < 2^{-k-2}$, and let $\langle q_n \rangle_n, \langle q'_n \rangle_n \subset \langle p_n \rangle_n$, $\forall n (\rho(q_n, x) < 2^{-n-2} \wedge \rho(q'_n, y) < 2^{-n-2})$, then there are γ, δ as in (1) such that $q_n = p_{\delta n}$ for all n , $x = x_\gamma$; and since

$\rho(q'_n, q'_{n+1}) < 2^{-n-1}$, $\rho(q_{k-1}, q'_k) \leq \rho(q_{k-1}, x) + \rho(x, y) + \rho(y, q'_k) < 2^{-k-1} + 2^{-k-2} + 2^{-k-2} = 2^{-k}$, there are also γ', δ' with $\delta'0 = \gamma'0$, $\delta'(n+1) = \alpha(n, \delta'n, \gamma'n)$, $\langle p_{\delta'n} \rangle_n = q_0, \dots, q_{k-1}, q'_k, q'_{k+1}, \dots$ and so $y = x_{\gamma'}$; since $\bar{\gamma}'k = \bar{\gamma}k$, $U(2^{-k-2}, x) \subset V_{\bar{\gamma}k}$.

5.17. Examples of complete separable metric spaces

(a) $\mathbb{R}, \mathbb{R}^n, [0, 1]$.

(b) If α, β are given we put

$$\mu_n(\alpha, \beta) = \sup\{2^{-i} : (i < n \wedge \alpha(i) \neq \beta(i)) \vee i = n\},$$

$\rho(\alpha, \beta) = \lim_n \mu_n(\alpha, \beta)$. ρ is a metric on $\mathbb{N}^{\mathbb{N}}$; this is the constructive equivalent of classical Baire space.

(c) This metric for Baire space obviously carries over to every subset of Baire space, hence in particular to the Cantor-set of 0–1-sequences.

(d) Hilbert space of countably infinite dimension.

6. Continuity; choice sequences

6.1. Continuity is more familiar than recursiveness, and, in the case of analysis and topology, also closer to the interests of mathematical practice. It is not surprising therefore that Brouwer's paradox: "all real-valued functions are continuous", and the underlying continuity postulates for choice sequences, received much attention — just as the continuity theorems of RA and CRA are among the most striking results in these areas.

In this section we shall briefly explain something of the original motivation behind the introduction of choice sequences, and show how this led to a theory of "continuous quantification" (choice sequences as a "figure of speech", see 6.3 and 6.14–6.16) with interesting metamathematical applications.

6.2. Heuristic considerations leading to the study of continuity schemata

First of all we observe that the usual classical examples of discontinuous functions defined on $\mathbb{R}$ are no counterexamples in intuitionistic mathematics. For example, consider the function f defined on $\mathbb{R}$ by $f(x) = 0$ for $x \leq 0$, $f(x) = 1$ for $x > 0$. From a constructive point of view this function is not everywhere defined; if x_0 is a real as defined in 5.8(4), i.e. $x_0 < 0 \vee x_0 = 0 \vee x_0 > 0$ is unknown, then we do not know how to compute $f(x_0)$ to any required degree of accuracy; that is to say, we are not able to prove that $f(x_0)$ is defined.

This example suggests that a real-valued function f , in order to be defined everywhere, should be such that approximations to the argument are sufficient to compute an approximation to the value with prescribed degree of accuracy — in short, f should be continuous. In other words, we expect that whenever $\forall x \in \mathbb{R} \exists! y \in \mathbb{R} A(x, y)$ is provable, there must be a *continuous* (in the standard topology of $\mathbb{R}$) f such that $\forall x \in \mathbb{R} A(x, fx)$.

As we shall see below in 6.4, $\forall \alpha \exists x$ -continuity (α ranging over number theoretic functions, x over natural numbers) is enough to ensure this.

It may be tempting to think of the following assumption: $\forall x \in \mathbb{R} \exists y \in \mathbb{R} A(x, y) \rightarrow \exists f \forall x \in \mathbb{R} A(x, fx)$ (f continuous in the standard topology of $\mathbb{R}$) as being equally plausible; but in fact in this case there is a counterexample.

Example. Constructively as well as classically, $x^3 - 3x + a = 0$ has a root in $\mathbb{R}$ for all $a \in \mathbb{R}$. However, it is easily seen, there is *no* $f: \mathbb{R} \rightarrow \mathbb{R}$, continuous in the standard topology for $\mathbb{R}$, such that $\forall a \in \mathbb{R} (f^3(a) - 3f(a) + a = 0)$.

On the other hand, an approximation to the root can be computed from an approximation to a , i.e. from an initial segment of a real number generator for a . The natural topology for r.n.g.'s is that of zero-dimensional Baire space (i.e. a neighbourhood consists of all r.n.g.'s which have a certain initial segment in common), and therefore we can rephrase the preceding assertion as: there is a continuous mapping (relative to Baire-space topology) assigning an r.n.g. for a root of $x^3 - 3x + a$ to each r.n.g. for a . Correspondingly, we shall see (in 6.13–6.16) that we can adopt a $\forall \alpha \exists \beta$ -continuity schema.

Note that the preceding example also illustrates “intensional aspects”: a method Φ determining a real y for each real x may use all available information about x ; and since a real is given to us as an r.n.g., Φ acts in fact on r.n.g.'s, and it is not necessary that $\langle r_n \rangle_n \sim \langle r'_n \rangle_n \rightarrow \Phi(\langle r_n \rangle_n) \sim \Phi(\langle r'_n \rangle_n)$.

Choice sequences. Brouwer's concept of choice sequence provides a sort of theoretical reason for the continuity schemata, which may be described as follows.

A proof of $\forall \alpha \exists x A(\alpha, x)$ implicitly contains an operation Φ such that $\forall \alpha A(\alpha, \Phi \alpha)$, but in the determination of $\Phi \alpha$ all available non-extensional information may be used (e.g. Gödel numbers if α ranges over total recursive functions). However, we may also consider “unfinished” sequences, i.e. processes for determining values to each argument which are not a priori determined by a law (extreme example: the sequence of the

casts of a die); expressed otherwise, we may enlarge (generalize) our concept of sequence by abstracting from the idea that a sequence should always be determined by a law, and we retain only the essential feature: to each argument n eventually a value αn will be determined. For this generalized concept, $\forall \alpha \exists x A(\alpha, x)$ becomes a much stronger assertion, since the range of α has been extended; and it is plausible that an operation Φ which should produce an x to *each* α (hence also in the extreme case where at any stage in the construction of α only an initial segment of α is known) is necessarily continuous, i.e. Φ should satisfy

$$\forall \alpha \exists x \forall \beta \in \bar{\alpha} x (\Phi \alpha = \Phi \beta)$$

which results in a continuity schema

$$\text{WC} - \text{N}^* \quad \forall \alpha \exists x A(\alpha, x, \gamma) \rightarrow \forall \alpha \exists y \exists x \forall \beta \in \bar{\alpha} y A(\beta, x, \gamma).$$

Assuming further that for a continuous operation Φ we can decide whether an initial segment $\bar{\alpha}x$ of the argument α is sufficient to compute $\Phi \alpha$ or not (which means that Φ is given to us by a neighbourhood function β such that $\beta(\bar{\alpha}x) \neq 0 \Leftrightarrow \Phi \alpha$ can be computed from $\bar{\alpha}x$ and has value $\beta(\bar{\alpha}x) \div 1$) we can strengthen $\text{WC} - \text{N}^*$ to $\text{C} - \text{N}^*$ or CONT_0

$$\text{CONT}_0 \quad \forall \alpha \exists x A(\alpha, x, \gamma) \rightarrow \exists \beta \in K_0 \forall \alpha A(\alpha, \beta(\alpha), \gamma)$$

where

$$K_0 \beta \equiv_{\text{def}} \forall \alpha \exists x (\beta(\bar{\alpha}x) \neq 0) \wedge \forall nm (\beta n \neq 0 \rightarrow \beta n = \beta(n * m)), \quad (1)$$

$$\beta(\alpha) = x \equiv_{\text{def}} \exists y (\beta(\bar{\alpha}y) = x + 1), \quad (2)$$

$$A(\alpha, \beta(\alpha), \gamma) \equiv_{\text{def}} \exists x (\beta(\alpha) = x \wedge A(\alpha, x, \gamma)). \quad (3)$$

Since most of the mathematical developments in elementary analysis do not depend on the assumption that the elements of $\mathcal{U}$ are given by a law, they should be valid for choice sequences (= the enlarged concept of a sequence as described above) as well; and for choice sequences it is plausible to assume in addition the continuity schema CONT_0 .

6.3. Elimination of choice sequences

However, our arguments made CONT_0 only plausible but did not justify it in a rigorous way. In fact, at present no simple concept of choice sequence is known for which both CONT_0 and the closure conditions on universes $\mathcal{U}$ given in 5.2 can be *derived*.

Therefore we shall follow another approach in 6.13–6.16 below: we shall justify quantification over choice sequences by reinterpretation. There are essentially two methods for doing this; the first one is Kleene's realizability

by functions, which is briefly discussed in 6.23; the other method consists in elimination of choice sequences by a method of contextual definition. More precisely, we consider formal systems containing, besides number quantifiers, two sorts of functional quantification: ordinary function quantifiers (“constructive function quantifiers”) and choice quantifiers. The meaning of the choice quantifiers is then explained by a contextual definition in terms of the other logical operators — they are explained as a “figure of speech”. The definition automatically validates CONT_0 ; most of the work consists in showing that the choice quantifiers indeed can be assumed to satisfy the ordinary quantifier laws (a fact which would have been obvious if we could have regarded quantification over choice sequences as a quantification over a special sort of objects).

Before we describe the elimination and its applications in 6.13–6.16, we shall first present (1) a mathematical application of $\text{WC} - \text{N}^*$ (for more illustrations of the use of $\text{WC} - \text{N}^*$ in mathematics see TROELSTRA [1977a], Ch. 6), (2) a brief discussion of the relation between Church’s thesis and continuity, and (3) some logical relationships relative to EL^* .

6.4. THEOREM. *Let $\Gamma = \langle V, \rho \rangle$ be a complete, separable, metric space constructed over the basis points $\langle p_n \rangle_n$; let $\{W_i : i \in I\}$, $I \subset \mathbb{N}$ be a covering of Γ , i.e. $\forall x \in V \exists i \in I (x \in W_i)$. Then $\{\text{Int}(W_i) : i \in I\}$ is again a covering of Γ ($\text{Int}(W) = \text{Interior of } W$), provided the universe $\mathcal{U}$ of number theoretic functions (see 5.2) satisfies $\text{WC} - \text{N}^*$.*

PROOF. Using the standard representation (5.16) for complete, separable, metric spaces, we have

$$\forall \alpha \exists i \in I (x_\alpha \in W_i).$$

By $\text{WC} - \text{N}^*$,

$$\forall \alpha \exists i \exists k \forall \beta \in \bar{\alpha} k (x_\beta \in W_i \wedge i \in I).$$

With the definition of $V_{\bar{\alpha}k}$ (see 5.10),

$$\forall \alpha \exists i \exists k (i \in I \wedge V_{\bar{\alpha}k} \subset W_i)$$

and thus with property (4) in 5.16,

$$\forall x \exists i \in I (x \in \text{Int}(W_i)). \quad \square$$

COROLLARY. *Let $\Gamma = \langle V, \rho \rangle$, $\Gamma' = \langle V', \rho' \rangle$ be complete, separable, metric spaces with basis points $\langle p_n \rangle_n$, $\langle p'_n \rangle_n$ respectively. Any mapping f from Γ into Γ' is continuous.*

PROOF. Let $U_i = \{x: \rho'(p'_i, fx) < 2^{-i}\}$, $i \in \mathbb{N}$ fixed; $\{U_i: i \in \mathbb{N}\}$ covers Γ . By the preceding theorem, $\{\text{Int}(U_i): i \in \mathbb{N}\}$ covers Γ , therefore

$$\forall x \in V \exists k \exists i (U(x, 2^{-k}) \subset U_i)$$

and thus for any x we can find k, i such that

$$\rho(x, y) < 2^{-k} \rightarrow fy \in U_i,$$

hence $\rho(fx, fy) \leq \rho(fx, p'_i) + \rho(fy, p'_i) < 2 \cdot 2^{-i}$. $\square$

6.5. Church's thesis and continuity

For $\mathcal{U} = \mathcal{R}$, the set of total recursive functions, $\text{WC} - \mathbf{N}^*$ is manifestly false since $\text{CT} \equiv \forall \alpha \exists x \{ \forall y \exists z (Txyz \wedge \alpha y = Uz) \}$ holds but x cannot be determined from an initial segment of α only: CT very forcefully asks attention for *intensional* aspects of sequences (namely their Gödel number). On the other hand, CT and

$$\text{CONT}_0! \quad \forall \alpha \exists! x A(\alpha, x) \rightarrow \exists \gamma \in K_0 \forall \alpha A(\alpha, \gamma(\alpha))$$

(K_0 defined as in 6.2(1)) are compatible, in fact $\mathbf{HA} + \mathbf{M} + \text{ECT}_0 \vdash \text{CONT}_0!$ More is true: in CRA (i.e. $\mathbf{HA} + \mathbf{M} + \text{ECT}_0$, cf. 4.13) the corollary of 6.4 is provable (see CEITIN [1959], MOSCHOVAKIS [1964]). However, in this case the corollary holds so to speak for quite different reasons: the condition that an operation, which is defined for all total recursive functions, is *extensional* (depends on the course of values of the functions only) is quite strong.

6.6–6.12. Some logical relationships relative to EL^* , bar induction

6.6. K_0 , the set of neighbourhood functions, has already been defined in 6.2(1). We put

$$K_1 \alpha \equiv_{\text{def}} \forall \gamma \exists z \forall \beta \leq \gamma (\alpha(\bar{\beta}z) \neq 0) \wedge \forall n m (\alpha n \neq 0 \rightarrow \alpha n = \alpha(n * m)). \quad (1)$$

$K_1 \alpha$ expresses that α is a neighbourhood function, and that the functional Φ_α

$$\Phi_\alpha \beta = x \leftrightarrow \exists z (\alpha(\bar{\beta}z) = x + 1)$$

represented by α is uniformly continuous on compact subsets of $\mathcal{U}$ (= the range of our function quantifiers).

We introduce K_2 by a generalized inductive definition

$$\text{K1-2} \quad A(\alpha, K_2) \rightarrow K_2 \alpha,$$

$$\text{K3} \quad \forall \alpha [A(\alpha, Q) \rightarrow Q\alpha] \rightarrow [K_2\alpha \rightarrow Q\alpha],$$

where

$$A(\alpha, P) \equiv_{\text{def}} \exists x (\alpha = \lambda n. Sx) \vee (\alpha 0 = 0 \wedge \forall x (\lambda n. \alpha(\hat{x} * n) \in P)). \quad (2)$$

K1–2 is in fact equivalent to the conjunction of

$$\text{K1} \quad \alpha = \lambda n. Sx \rightarrow K_2\alpha,$$

$$\text{K2} \quad \alpha 0 = 0 \wedge \forall x (\lambda n. \alpha(\hat{x} * n) \in K_2) \rightarrow K_2\alpha.$$

K1 and K2 express that K_2 satisfies certain closure conditions, K3 that K_2 is the minimal set satisfying those closure conditions.

We note in passing that generalized inductive definitions are regarded as an acceptable method of definition in most forms of constructivism (not in finitism), e.g. in intuitionism, CRA (MARKOV [1974]) and strict constructivism.

Classically $K_0 \subset K_2$. To see this, note first that for any $\beta \in K_0 - K_2$, $\beta 0 = 0$ (since otherwise $\beta = \lambda n. \beta 0 \in K_2$ by K1) and also $\exists x (\lambda n. \beta(\hat{x} * n) \in K_0 - K_2)$. Thus, if $\alpha \in K_0 - K_2$, there exists by an axiom of dependent choices a γ such that $\forall x (\lambda n. \alpha(\hat{\gamma}x * n) \in K_0 - K_2)$, and thus $\forall x (\alpha(\hat{\gamma}x) = 0)$; but this conflicts with $\alpha \in K_0$ since this implies $\forall \gamma \exists x (\alpha(\hat{\gamma}x) \neq 0)$.

The converse $K_2 \subset K_0$ also holds constructively: apply K3 with $Q\alpha \equiv \forall \beta \exists x (\alpha(\hat{\beta}x) \neq 0)$ and with $Q\alpha \equiv \forall nm (\alpha n \neq 0 \rightarrow \alpha n = \alpha(n * m))$.

Brouwer's "bar theorem" amounted to accepting $K_0 = K_2$ also intuitionistically. (For an extensive discussion see TROELSTRA [1977a].) We can prove more than $K_2 \subset K_0$, namely:

6.7. LEMMA. $K_2 \subset K_1$.

PROOF. Apply K3 with $K_1\alpha$ for $Q\alpha$. $\square$

The next lemma and theorem give us an axiomatization equivalent to K1–3.

LEMMA (Induction over unsecured sequences). *In $\text{EL}^* + \text{K1–3}$ we can derive*

$$\text{IUS} \quad K_2\alpha \rightarrow [\forall n (\alpha n \neq 0 \rightarrow Q'n) \wedge \forall n (\forall y Q'(n * \hat{y}) \rightarrow Q'n) \rightarrow Q'(\quad)].$$

PROOF. Apply K3 to

$$Q\alpha \equiv \forall m [\forall n (\alpha n \neq 0 \rightarrow Q'(m * n)) \wedge \forall n (\forall y Q'(m * n * \hat{y}) \rightarrow \rightarrow Q'(m * n)) \rightarrow Q'm];$$

this yields the assertion of the lemma if we take $m = \langle \quad \rangle$. $\square$

6.8. THEOREM. $IUS + \forall \alpha (K_2\alpha \rightarrow \forall nm (\alpha n \neq 0 \rightarrow \alpha n = \alpha(n * m))) + K1-2$ is deductively equivalent to $K3$ relative to EL^* .

PROOF. $K1, 2$ are easy. To establish $K3$, we show that under the hypotheses $\forall \alpha (A(\alpha, Q) \rightarrow Q\alpha)$ and $K_2\alpha$, $Q\alpha$ holds; this can be done by application of IUS to $Q'n \equiv \lambda m. \alpha(n * m) \in K_2$. $\square$

Kleene formulated (e.g. in KLEENE and VESLEY [1965]) Brouwer's "bar theorem" (induction over the partial ordering of a well-founded tree) as:

$$BI_D \quad \forall \alpha \exists x P(\bar{\alpha}x) \wedge \forall n (Pn \vee \neg Pn) \wedge \forall n (Pn \rightarrow Qn) \wedge \wedge \forall n (\forall y Q(n * \hat{y}) \rightarrow Qn) \rightarrow Q(\quad).$$

A slightly stronger form is:

$$BI \quad \forall \alpha \exists x P(\bar{\alpha}x) \wedge \forall nm (Pn \rightarrow P(n * m)) \wedge \forall n (Pn \rightarrow Qn) \wedge \wedge \forall n (\forall y Q(n * \hat{y}) \rightarrow Qn) \rightarrow Q(\quad).$$

6.9. THEOREM. $EL^* + K1-3 \vdash K_0 = K_2 \rightarrow BI_D$.

PROOF. Let

$$\forall \alpha \exists x P(\bar{\alpha}x), \tag{3}$$

$$\forall n (Pn \rightarrow Qn), \tag{4}$$

$$\forall n (Pn \vee \neg Pn), \tag{5}$$

$$\forall n (\forall y Q(n * \hat{y}) \rightarrow Qn). \tag{6}$$

Since P is decidable, the function β defined by

$$\beta n = 1 \iff \exists m < n Pm,$$

$$\beta n = 0 \text{ otherwise}$$

is an element of K_0 by virtue of (3). Now put

$$Q'n \equiv_{\text{def}} Qn \vee \exists m < n Pm$$

and assume $\forall y Q'(n * \hat{y})$. If $\exists m < n Pm$, or Pn , then $Q'n$ (by the definition

of $Q'n$ and (4)). Assuming $\neg \exists m \leq n Pm$, i.e. $\neg \exists m < n * \hat{y}. Pm$ for all y , then by $\forall y Q'(n * \hat{y})$, $\forall y Q(n * \hat{y})$, hence with (6) Qn and thus $Q'n$.

We have now shown

$$\exists m \leq n Pm \vee \neg \exists m \leq n Pm \rightarrow (\forall y Q'(n * \hat{y}) \rightarrow Q'n)$$

and therefore by (5) also

$$\forall y Q'(n * \hat{y}) \rightarrow Q'n.$$

It is also obvious that

$$\beta n \neq 0 \rightarrow Q'n$$

and so with the lemma on IUS, and $K_0 = K_2$ we find $Q'0$, hence $Q0$ since $\exists m < 0 Pm$ is excluded. $\square$

6.10. THEOREM. *Relative to $\mathbf{EL}^* + \text{CONT}_0$, BI_D is deductively equivalent to BI.*

PROOF. Assume BI_D , (3), (4), (6) and

$$\forall nm (Pn \rightarrow P(n * m)). \quad (7)$$

By CONT_0 there is a $\beta \in K_0$ such that

$$\forall \alpha P(\bar{\alpha}(\beta(\alpha))).$$

We put

$$P'n \equiv_{\text{def}} \beta n \neq 0 \wedge \text{lh}(n) \geq \beta n \div 1.$$

Then obviously $\forall \alpha \exists x P' \bar{\alpha} x$, and since (by (7)) $P'n \rightarrow Pn$, also $\forall n (P'n \rightarrow Qn)$; $\forall n (P'n \vee \neg P'n)$ is also obvious, and therefore with BI_D , $Q0$ follows. $\square$

6.11. THEOREM. *Relative to $\mathbf{EL}^* + \text{CONT}_0$, BI is deductively equivalent to transfinite induction*

$$\text{TI} \quad \forall \alpha \exists x \neg (\alpha x < \alpha(x+1)) \rightarrow [\forall x (\forall y < x Qy \rightarrow Qx) \rightarrow \forall x Qx]$$

($<$ a relation definable in $\mathbf{EL}^*$).

Relative to $\mathbf{EL}^$, the schemata TI_D (TI restricted to decidable Q) and BI_D are equivalent.*

PROOF. See HOWARD and KREISEL [1966], Corollary 1 to Theorem 5B, and Theorem 6B. $\square$

The following theorem is similar to $K_0 = K_2 \rightarrow \text{BI}_D$ derived above

6.12. THEOREM. $\mathbf{EL}^* \vdash K_0 = K_1 \rightarrow \mathbf{FAN}_D$, where $\mathbf{FAN}_D$ is the schema $\mathbf{FAN}_D \quad \forall \alpha \exists x A(\bar{\alpha}x) \wedge \forall n (An \vee \neg An) \rightarrow \exists z \forall \beta \leq \lambda x. 1 \exists x \leq z A(\bar{\beta}x)$.

We leave the proof to the reader.

6.13–6.16. Elimination of choice sequences

6.13. Description of the systems $\mathbf{CS}_H$, $\mathbf{CS}_H$, $\mathbf{CS}$

The developments in this and the next two subsections are necessarily sketchy at some places, but sufficiently detailed, we trust, to give a good impression of the methods used. For full details see KREISEL and TROELSTRA [1970], and TROELSTRA [1974].

In the discussion below we shall consider theories $\mathbf{H}$ in a language $L[\mathbf{H}]$; $L[\mathbf{H}]$ contains (1) numerical variables; (2) constructive function variables (a, b, c, d); (3) variables for the elements of a certain class K of neighbourhood functions (K -variables; $e, f, e', \dots$).

Note. If K is a constant definable in $\mathbf{H}$ (without the use of K -variables), then the addition of K -variables produces systems which are definitional extensions of systems without K -variables.

Furthermore $L[\mathbf{H}]$ contains

- (i) all constants of $\mathbf{EL}$,
- (ii) certain constants for elements of K ,
- (iii) certain constants for operators of types $\mathbf{N} \rightarrow K$, $K^2 \rightarrow K$, $K^2 \rightarrow K$ (notably $k, ;, :$). The presence of such constants together with their defining axioms implicitly expresses certain closure properties of K .
- (iv) K -abstraction, indicated by λ' : if ϕ is a K -term ($= K$ -functor) and t a numerical term, then $\lambda' n. \phi(\langle t \rangle * n)$ is again a K -functor.
- (v) operations $|\cdot|, \cdot, \cdot$ with the following rule of term-formation: if ϕ is a K -functor, ϕ' a functor, then $\phi \mid \phi'$ is a functor ($=$ function term), $\phi(\phi')$ a numerical term.

The systems $\mathbf{H}$ considered are axiomatized on the basis of many-sorted intuitionistic predicate logic, all the axioms and axiom schemata of $\mathbf{EL}$ and in addition $\mathbf{AC}_{01} \equiv \mathbf{AC} - \mathbf{NF}$.

$$\mathbf{AC} - \mathbf{NF} \quad \forall x \exists a A(x, a) \rightarrow \exists b \forall x A(x, (b)_x).$$

There are axioms for the elements of K (varying in the different applications) implying

$$\begin{cases} \forall e \forall b \exists x (e(\bar{b}x) \neq 0), \\ \forall nm (en \neq 0 \rightarrow en = e(n * m)), \end{cases} \quad (1)$$

i.e. the elements of K are neighbourhood functions on the range of the function variables. (1) justifies the introduction of axioms

$$e(a) = x \leftrightarrow \exists y (e(\bar{a}y) = x + 1), \quad (2)$$

$$(e \mid a)(x) = y \leftrightarrow \exists z (e(\hat{x} * \bar{a}z) = y + 1). \quad (3)$$

(2) and (3) show that the introduction of the operations $.(.)$ and $.\mid$ amounts to a definitional extension; the reason for introducing K -variables is that this permits us to regard $.(.)$ and $.\mid$ as total operations provided the range of the first argument is restricted to K -functions. For $\lambda'x$ we have

$$(\lambda'n. e(\hat{x} * n))t = e(\hat{x} * t). \quad (4)$$

With every element e of K we can associate two continuous functionals $\Phi_e : \mathbb{N}^{\mathbb{N}} \rightarrow \mathbb{N}$ and $\Psi_e : \mathbb{N}^{\mathbb{N}} \rightarrow \mathbb{N}^{\mathbb{N}}$ such that

$$\Phi_e(a) = e(a), \quad \Psi_e(a) = e \mid a.$$

For the proof of the elimination theorems and their applications K has to satisfy certain closure conditions which must be derivable from the axioms for K in $\mathbf{H}$.

A complete list of these closure conditions CC is irrelevant for our purposes. For a list CC which is in any case sufficient for the applications discussed below, see TROELSTRA [1974]. Among other things, CC expresses closure under certain primitive recursive operations $;$, $:$, $\wedge$ such that

$$(e;f)(a) = e(f \mid a), \quad (e:f) \mid a = e \mid (f \mid a), \quad (e \mid a)(f \mid a) = (e \wedge f)(a),$$

i.e.

$$\Phi_{e;f}a = \Phi_e(\Psi_f a), \quad \Psi_{e:f}a = \Psi_e(\Psi_f a), \quad \Phi_{e \wedge f}a = (\Psi_e a)(\Psi_f a).$$

We also need an operator mapping sequences onto sequences with initial segment n . Let $k(n, m)$ be a function such that

$$\begin{cases} m = \hat{x} * m' \wedge x < \text{lth}(n) \rightarrow k(n, m) = (n)_x, \\ m = \hat{x} * m' \wedge x \geq \text{lth}(n) \wedge \text{lth}(m') > x \rightarrow k(n, m) = (m')_x, \\ k(n, m) = 0 \text{ in all other cases.} \end{cases}$$

We shall assume CC to be such that $\lambda m. k(n * m) \in K$; assuming that in $L[\mathbf{H}]$ $k^{(t)}$ is a K -term for each t such that in $\mathbf{H}$ $k^{(n)}m = k(n, m)$, we may introduce the abbreviation

$$n \mid a \equiv_{\text{def}} k^{(n)} \mid a.$$

Obviously,

$$\begin{aligned} n \mid a \in n, \quad a \in n \rightarrow n \mid a = a, \\ (n \mid a)(x) = ax \quad \text{for } x \geq \text{lth}(n). \end{aligned}$$

Now a system **H** may be embedded in a corresponding theory $\mathbf{CS}_H^-$ as follows. The language of $\mathbf{CS}_H^-$ contains choice variables $\alpha, \beta, \gamma, \delta$, and the rules of term-formation of **H** are extended in an obvious way:

(1) If t is a numerical term, ϕ a choice functor, then ϕt is a numerical term.

(2) If ϕ is a K-functor, ϕ' a choice functor, then $\phi \mid \phi'$ is a choice functor, and $\phi(\phi')$ a numerical term.

(3) If t is a term, then $\lambda''x.t$ is a choice functor.

In $\mathbf{CS}_H$, λ is restricted in an obvious manner: λ is only to be applied to terms not containing choice parameters. The reason for distinct abstraction operators $\lambda, \lambda', \lambda''$ is that we wish to keep functors, K-functors, choice-functors syntactically distinct. (For a complete description of the rules of term-formation, see KREISEL and TROELSTRA [1970].)

Convention. In writing $A(\alpha_1, \dots, \alpha_n)$ etc. for a formula with parameters $\alpha_1, \dots, \alpha_n$, we shall assume *all* the choice parameters to be contained among $\alpha_1, \dots, \alpha_n$.

To the axioms of **H** we add

$$\begin{aligned} A1 \quad & \forall \alpha \exists x (e(\bar{a}x) \neq 0), \\ A2 \quad & \forall \alpha \exists \beta A(\alpha, \beta) \rightarrow \exists e \forall \alpha A(\alpha, e \mid \alpha), \\ A3 \quad & \forall \alpha (A\alpha \rightarrow B\alpha) \rightarrow \forall e [\forall \alpha A(e \mid \alpha) \rightarrow \forall \alpha B(e \mid \alpha)]. \end{aligned}$$

To obtain the system $\mathbf{CS}_H$ we add also

$$\begin{aligned} A4 \quad & \forall \alpha \exists a A(\alpha, a) \rightarrow \\ & \rightarrow \exists e \exists b \forall n (en \neq 0 \rightarrow \forall \alpha A(n \mid \alpha, \lambda m. b((en \div 1) * m))). \end{aligned}$$

Using closure conditions on K we can show this to imply

$$\forall \alpha \exists e A(\alpha, e) \rightarrow \exists e \exists f \forall n (en \neq 0 \rightarrow \forall \alpha A(n \mid \alpha, \lambda' m. f((en \div 1) * m))).$$

By predicate logic, the implication in A3, A4 also holds in the other direction. We remark

(i) A2 implies various forms of $\forall \alpha \exists x$ -continuity such as

$$\forall \alpha \exists x A(\alpha, x) \leftrightarrow \exists e \forall \alpha A(\alpha, e(\alpha)),$$

$$\forall \alpha \exists x A(\alpha, x) \leftrightarrow \exists e \forall n (en \neq 0 \rightarrow \forall \alpha A(n \mid \alpha, en \div 1)).$$

Note that $\forall \alpha A(n \mid \alpha, en - 1) \leftrightarrow \forall \alpha \in n A(\alpha, en \div 1)$. We leave it to the reader to derive these forms from A2.

(ii) Another corollary of A2 is the “specialization principle”,

$$\text{SP} \quad \exists \alpha A \alpha \rightarrow \exists a A (\lambda "x. ax)$$

($A\alpha$ not containing choice parameters besides α). To see this, note that $\exists \alpha A \alpha$ implies $\forall \beta \exists \alpha A \alpha$, hence by A2, $\forall \beta A(e \mid \beta)$ for some e , and therefore $A(e \mid \lambda "x. 0)$.

(iii) It is also not hard to show that

$$\forall \alpha A \alpha \leftrightarrow \forall a A a$$

for A prime, since the truth of $A\alpha$ for A prime depends on finite initial segments of α : since $\forall \alpha (A\alpha \vee \neg A\alpha)$, i.e. $\forall \alpha \exists x [(x = 0 \wedge A\alpha) \vee (x = 1 \wedge \neg A\alpha)]$ it follows that $\exists e \forall n (en \neq 0 \rightarrow (\forall \alpha \in n A\alpha) \vee (\forall \alpha \in n \neg A\alpha))$. Therefore, if $\forall a A a$, $\forall \alpha \in n \neg A\alpha$ is excluded for all n , and thus $\exists e \forall n (en \neq 0 \rightarrow \forall \alpha \in n A\alpha)$ which in view of $\forall \alpha \exists x (e(\bar{\alpha}x) \neq 0)$ implies $\forall \alpha A \alpha$.

6.14. Description of the elimination mapping τ

The description is by induction on the number of logical operators within the scope of a choice quantifier (including the choice quantifiers themselves); we assume $\vee$ to have been eliminated beforehand by the use of $(A \vee B) \leftrightarrow \exists x [(x = 0 \rightarrow A) \wedge (x \neq 0 \rightarrow B)]$. We define an auxiliary mapping $\mapsto$ for formulae starting with $\forall \alpha, \exists \alpha$ and not containing any choice parameters free. The general idea behind the definition of τ is to push choice quantifiers inwards as far as possible.

- (i) $\exists \alpha A \alpha \mapsto \exists a A a$,
- (ii) $\forall \alpha A \alpha \mapsto \forall a A a$ for A prime,
- (iii) $\forall \alpha (A \alpha \wedge B \alpha) \mapsto \forall \alpha A \alpha \wedge \forall \alpha B \alpha$,
- (iv) $\forall \alpha (A \alpha \rightarrow B \alpha) \mapsto \forall e (\forall \alpha A(e \mid \alpha) \rightarrow \forall \alpha B(e \mid \alpha))$,
- (v) $\forall \alpha \exists x A(\alpha, x) \mapsto \exists e \forall n (en \neq 0 \rightarrow \forall \alpha A(n \mid \alpha, en \div 1))$,
- (vi) $\forall \alpha \exists \beta A(\alpha, \beta) \mapsto \exists e \forall \alpha A(\alpha, e \mid \alpha)$,
- (vii) $\forall \alpha \forall x A(\alpha, x) \mapsto \forall x \forall \alpha A(\alpha, x)$,
 $\forall \alpha \forall a A(\alpha, a) \mapsto \forall a \forall \alpha A(\alpha, a)$,
 $\forall \alpha \forall e A(\alpha, e) \mapsto \forall e \forall \alpha A(\alpha, e)$,
- (viii) $\forall \alpha \forall \beta A(\alpha, \beta) \mapsto \forall e \forall f \forall \alpha A(e \mid \alpha, f \mid \alpha)$,
- (ix) $\forall \alpha \exists a A(\alpha, a) \mapsto$
 $\mapsto \exists e \exists b \forall n (en \neq 0 \rightarrow \forall \alpha A(n \mid \alpha, \lambda n. b((en \div 1) * n)))$,
 $\forall \alpha \exists e A(\alpha, e) \mapsto$
 $\mapsto \exists e \exists f \forall n (fn \neq 0 \rightarrow \forall \alpha A(n \mid \alpha, \lambda' n. f((en \div 1) * n)))$.

Applying $\mapsto$ as often as possible we end up with a formula not containing

any choice variables or quantifiers; we denote the result of this process applied to A by $\tau(A)$.

Note. (1) Formulae of $\mathbf{H}$ are left unchanged by τ .

(2) The clauses (i)–(viii) in the definition of $\mapsto$ suffice to define τ for all A which do not contain quantifiers $\exists e, \exists a$ within the scope of a universal choice quantifier, and do not contain choice parameters.

From the definitions and remarks in 6.13–6.14 we obtain:

6.15. FIRST ELIMINATION THEOREM. (i) *If A does not contain quantifiers $\exists a, \exists e$ within the scope of a universal choice quantifier, then*

$$\mathbf{CS}_H^- \vdash A \leftrightarrow \tau(A).$$

(ii) *In $\mathbf{CS}_H$, for formulae not containing choice parameters free,*

$$\mathbf{CS}_H \vdash A \leftrightarrow \tau(A).$$

PROOF. At each step $\mapsto$ replaces a (sub-)formula by an equivalent formula, as can be seen by inspection of the clauses of the definition of τ , taking into account the various consequences of A1–A4 noted in the preceding subsection. $\square$

But we have more:

6.16. SECOND ELIMINATION THEOREM.

$$\mathbf{H} \vdash \tau(A) \Leftrightarrow \mathbf{CS}_H \vdash A.$$

PROOF. By induction on the length of derivations in $\mathbf{CS}_H$. See KREISEL and TROELSTRA [1970], §7. $\square$

These theorems permit us to treat the choice quantifiers in $\mathbf{CS}_H$ as a “figure of speech” which can be fully explained relative to $\mathbf{H}$.

6.17–6.22. Some applications

6.17. Let $\mathbf{H}^*$ be the system corresponding to $\mathbf{H}$, but written with variables $\alpha, \beta, \gamma, \delta$ instead of a, b, c, d . Let Γ be a set of additional postulates, Γ^* their transcription in the language of $\mathbf{H}^*$. Let us assume

$$\mathbf{H}^* + \Gamma^* \subseteq \mathbf{CS}_H^-.$$

For sentences A of $\mathbf{CS}_H$ not containing quantifiers $\exists a, \exists e$ within the scope of choice quantifiers,

$$\mathbf{CS}_H \vdash A \Leftrightarrow \mathbf{H} \vdash \tau(A).$$

If A^* denotes the rewriting of $A \in L[\mathbf{H}]$ into $L[\mathbf{H}^*]$, and if

$$\mathbf{H} + \Gamma \vdash A,$$

then also

$$\mathbf{H}^* + \Gamma^* \vdash A^*$$

hence

$$\mathbf{CS}_H \vdash A^*$$

and therefore $\mathbf{H} \vdash \tau(A^*)$. For arithmetical A , $A^* \equiv A \equiv \tau(A^*)$, and therefore $\mathbf{H} + \Gamma$ is conservative over $\mathbf{H}$. This observation is used in the following two applications:

6.18. THEOREM. $\mathbf{EL} + \text{CONT}_1$ is conservative over $\mathbf{EL} + \text{AC-NF}$ w.r.t. arithmetical sentences. Here CONT_1 is $\forall a \exists b A(a, b) \rightarrow \exists e \in K_0 \forall a A(a, e \mid a)$.

PROOF. Let $\mathbf{H}$ be a rewriting of $\mathbf{EL} + \text{AC-NF}$ in the language $L[\mathbf{H}]$ as described above, and let $K = K_0$ be the axioms for K ; then apply the preceding observation. $\square$

6.19. THEOREM. $\mathbf{EL} + \text{CONT}_1 + \text{FAN}$ is conservative over $\mathbf{EL} + \text{AC-NF}$ w.r.t. arithmetical sentences. Here FAN is

$$\begin{aligned} \text{FAN} \quad & \forall a \leq \lambda x.1 \exists x A(\bar{a}x) \rightarrow \\ & \rightarrow \exists z \forall a \leq \lambda x.1 \exists y \forall b \leq \lambda x.1 (\bar{a}z = \bar{b}z \rightarrow A(b, y)). \end{aligned}$$

PROOF. Similar to the preceding theorem, but now the axioms for K are $K = K_1$. $\square$

Remark. In view of a result of GOODMAN [1968] (also proved, by different methods, in MINC [1975]), that $\mathbf{EL} + \text{AC-NF}$ is conservative over $\mathbf{HA}$, the conclusion in Theorems 6.18 and 6.19 may be strengthened to conservativeness over $\mathbf{HA}$.

6.20. THEOREM. IDB_1 is the theory $\mathbf{H}$ with axioms $K = K_2$ for K . Then $\mathbf{CS}_{\text{IDB}_1} = \mathbf{CS}$ is conservative over IDB_1 .

PROOF. Apply the second elimination theorem. $\square$

Note also that if A does not contain $\vee, \exists$ within the scope of a universal function quantifier, one easily verifies $\mathbf{H} \vdash \tau(A^*) \leftrightarrow A$ (A^* as before the result of rewriting a formula A of $\mathbf{H}$ in the language of $\mathbf{H}^*$). The proof is by induction on the number of logical operators within the scope of a universal function quantifier in A ; the preceding applications in Theorems 6.18 and 6.19 permit a slight strengthening by this remark.

6.21. THEOREM. *Let $\mathbf{FIM}$ be the system axiomatized as*

$$\mathbf{EL} + \mathbf{AC-NF} + \mathbf{BI} + \mathbf{CONT}_1$$

($\mathbf{FIM}$ is essentially the system of KLEENE and VESLEY [1965]); $\mathbf{CS}$ is a conservative extension of $\mathbf{FIM}$.

PROOF. $(\mathbf{IDB}_1)^*$ is a subsystem of $\mathbf{FIM}$, if we define K as K_0 , the set of neighbourhood functions (see 6.2(1)).

If we take any sentence A in the language of $\mathbf{FIM}$ such that $\mathbf{CS} \vdash A$, then

$$\mathbf{IDB}_1 \vdash \tau(A)$$

while on the other hand, since $\mathbf{FIM} \vdash (\tau(A))^*$, and $\mathbf{FIM} \vdash (\tau(A))^* \leftrightarrow A$ (since A did not contain quantifiers $\exists e, \exists a$, there was no need to use the postulate $A4$ in proving this equivalence) it follows that $\mathbf{FIM} \vdash A$. $\square$

6.22. For future use we note the following lemma, the proof of which is left to the reader:

LEMMA. *Let $\mathbf{CS} \vdash \forall \alpha [\forall x A(x, \alpha) \rightarrow \forall u \exists v B(u, v, \alpha)]$, A, B quantifier-free, α the only choice parameter in A, B . Then, with $\mathbf{IDB}_1$ as in 6.20,*

$$\mathbf{IDB}_1 \vdash \forall a [\forall x A(x, a) \rightarrow \forall u \exists v B(u, v, a)].$$

6.23. Realizability by functions

Kleene gave a reinterpretation for the system $\mathbf{FIM}$ (defined in Theorem 6.20 of the previous subsection) by means of realizability which interprets $\mathbf{FIM}$ in $\mathbf{B}$ (essentially $\mathbf{EL}^* + \mathbf{AC-NF} + \mathbf{BI}$), the basic system which is also compatible with classical logic (see KLEENE [1969], and KLEENE and VESLEY [1965]).

The definition is based on continuous function-application $\cdot | \cdot$ instead of partial-recursive function-application:

$$\alpha | \beta \approx \gamma \equiv_{\text{def}} \forall x (\alpha(\hat{x} * \bar{\beta} \min_z [\alpha(\hat{x} * \bar{\beta} z) \neq 0]) \dot{\div} 1 = \gamma x).$$

If we define “almost-negative” as before, but now permitting also existential function quantifiers, and we write “ α realizes $A(\beta_1, \dots, \beta_n)$ in this new sense” as “ $\alpha \mathbf{r}^1 A(\beta_1, \dots, \beta_n)$ ” then we can formulate a characterization theorem similar to 4.8.

THEOREM. (i) *For almost negative A , $\mathbf{EL}^* \vdash A \leftrightarrow \exists \alpha (\alpha \mathbf{r}^1 A)$.*

(ii) *Let the schema of generalized continuity GC be defined as*

$$\text{GC} \quad \forall \alpha [A\alpha \rightarrow \exists \beta B(\alpha, \beta)] \rightarrow \exists \gamma \forall \alpha [A\alpha \rightarrow !\gamma \mid \alpha \wedge B(\alpha, \gamma \mid \alpha)]$$

with A almost negative, $!\gamma \mid \alpha$ expressing $\exists \delta (\gamma \mid \alpha \approx \delta)$. Then

$$\mathbf{EL}^* + \text{GC} \vdash A \leftrightarrow \exists \alpha (\alpha \mathbf{r}^1 A) \quad \text{for all } A,$$

and

$$\mathbf{H} + \text{GC} \vdash A \Leftrightarrow \mathbf{H} \vdash \exists \alpha (\alpha \mathbf{r}^1 A) \quad \text{for } \mathbf{H} = \mathbf{EL}^*, \mathbf{EL}^* + \text{BI}, \mathbf{EL}^* + \text{FAN}.$$

7. Lawless sequences

7.1. In the preceding section we only presented a rough intuitive plausibility argument for the continuity axioms for choice sequences, and then proceeded to the treatment of choice sequences as a “figure of speech”. At present, no really satisfactory concept of choice sequence satisfying the axioms of **CS** is known — for a discussion of this problem, we refer to TROELSTRA [1977a], Appendix C.

There is one example of a simple concept of sequence (not a priori determined by a law) where it is possible to give an informal, but rigorous justification of the axioms (including continuity axioms): lawless sequences. The concept is meaningful from an intuitionistic viewpoint, but is of course illegitimate from the point of view of CRA.

Lawless sequences are most easily described as follows. We think of a lawless sequence as a process of determining values, such that eventually, for any given natural number, a corresponding term (value) of the sequences will be determined; at any given stage however, only finitely many terms of the sequence have been defined. We postulate that to each prescribed finite sequence n there is a lawless sequence starting with n . Of course, one may also consider sequences lawless relative to a given (lawlike) finitely branching tree: i.e. we know a priori that the sequence will be an infinite branch of the tree, but otherwise the sequence is lawless. A good “model” for a lawless sequence (with values x , $1 \leq x \leq 6$) is provided by the sequence of the casts of a die, provided we permit at the beginning a

finite number of deliberate placings of the die. Different lawless sequences may be identified in the model with different dice.

7.2. Some principles which can be shown to be valid for lawless sequences are (using ε , η as variables for lawless sequences)

$$A\varepsilon \rightarrow \exists n [\varepsilon \in n \wedge \forall \eta \in n A\eta], \quad (1)$$

$$\forall \varepsilon \exists x A(\varepsilon, x) \rightarrow \exists e \in K_{LS} \forall \varepsilon A(\varepsilon, e(\varepsilon)), \quad (2)$$

where

$$e \in K_{LS} \equiv_{\text{def}} \forall \varepsilon \exists x (e(\bar{\varepsilon}x) \neq 0) \wedge \forall nm (en \neq 0 \rightarrow en = e(n * m))$$

and the “extension principle”

$$e \in K_{LS} \rightarrow \forall a \exists x (e(\bar{a}x) \neq 0). \quad (3)$$

As stated in 7.1, we also postulate

$$\forall n \exists \varepsilon (\varepsilon \in n). \quad (4)$$

Let us consider for instance (1). Suppose we have a proof of $A\varepsilon$; since this proof must be completed at a certain stage, it must depend exclusively on our knowledge of the initial segment of ε known at that stage, say n ; hence the property A should equally hold for all lawless η with initial segment n .

(2) can be justified in the spirit of 6.2, but now even more convincingly, since for *all* lawless sequences, at any stage, only an initial segment is known.

(3) expresses that neighbourhood functions for type $\mathbb{N}^{\mathbb{N}} \rightarrow \mathbb{N}$ functionals on lawless sequences automatically extend to functionals defined on lawlike sequences as well. For a discussion of the extension principle see TROELSTRA [1977a], 2.11.

Remark. (i) Note that the justification of (1) is given, quite naturally, in subjectivistic terms (“what does the idealized mathematician know at a certain stage”). The justification of the axioms for lawless sequences is discussed at much greater length in Ch. 2 of TROELSTRA [1977a]. The justification of (i) also provides another example of a derivation of axioms by reflection on abstract concepts.

(ii) The interest of the lawless sequences is not only pedagogical; although we have introduced them here mainly to demonstrate the possibility of deriving rigorously axioms for a concept of sequence which is an “incomplete object”, and to show the use of the subjectivistic interpretation, they have other uses besides: (1) the construction of universes of

sequences which are suitable for (real-valued) analysis (cf. Ch. 4 of TROELSTRA [1977a]); and (2) in the discussion of validity and completeness of intuitionistic predicate logic (see Section 9, and TROELSTRA [1977b]; [1977a], Ch. 7).

8. Markov's principle

8.1. Considerable interest attaches to "Markov's schema" which can be stated as

$$M \quad \forall x (Ax \vee \neg Ax) \wedge \neg \neg \exists x Ax \rightarrow \exists x Ax$$

(A containing numerical parameters only) and its variants and weakenings. We may paraphrase M as follows: suppose A to be a predicate of natural numbers which can be tested for each number; and we know by indirect arguments that there should be an x such that Ax ; then we also believe that a computer with unbounded memory (or an algorithm) asked to search for an x such that Ax will eventually find one (given enough time). This paraphrase does not fit the variant where we permit e.g. choice sequences as parameters; and in fact, since M was first considered in the context of CRA (cf. MARKOV [1962]), its origin is purely mechanistic.

Nevertheless, there are interesting problems connected with the validity of (the analogue of) M where non-numerical parameters are present, so we shall also discuss (in Section 8.3)

$$M(\mathcal{U}) \quad \forall \alpha [\neg \neg \exists x (\alpha x = 0) \rightarrow \exists x (\alpha x = 0)]$$

where α is supposed to range over a universe $\mathcal{U}$ of sequences.

Note that M itself, in the presence of CT_0 , is equivalent to the special form

$$M_{PR} \quad \forall xy [\neg \neg \exists z Txyz \rightarrow \exists z Txyz]$$

or equivalently

$$\neg \neg \exists x Ax \rightarrow \exists x Ax \quad (A \text{ primitive recursive}).$$

8.2. Mathematical consequences of M and $M(\mathcal{U})$

An easy consequence, which considerably simplifies the theory of reals and real-valued functions, is given by the following:

THEOREM. *For reals ranging over $\mathbb{R}(\mathcal{U})$,*

$$\forall x (x \neq 0 \leftrightarrow x \# 0) \leftrightarrow M(\mathcal{U}).$$

Remark. In the presence of AC – NN! (= AC₀₀!),

$$\forall x \exists ! y A(x, y) \rightarrow \exists a \forall x A(x, ax)$$

$M(\mathcal{U})$ is equivalent to the variant of M where parameters ranging over $\mathcal{U}$ are permitted.

PROOF. Let $x \in \mathbb{R}(\mathcal{U})$, $\langle r_{an} \rangle_n \in x$, $x \neq 0$, $\forall k (|x - r_{ak}| < 2^{-k})$. Since $x \neq 0$, $\neg \forall k (|r_{ak}| < 2^{-k})$, hence $\neg \forall k \neg (|r_{ak}| \geq 2^{-k})$. $|r_{ak}| \geq 2^{-k}$ is expressible by a quantifier-free statement in the language of **EL**, so by QF – AC there is a b such that $bk = 0 \leftrightarrow (|r_{ak}| \geq 2^{-k})$; with M , $\exists k (|r_{ak}| \geq 2^{-k})$. $|x - r_{ak}| < 2^{-k} - 2^{-n}$ for a suitable n , hence $|x| \geq ||r_{ak}| - |x - r_{ak}|| > 2^{-n}$, so $x \neq 0$.

Conversely, if $\forall x (x \neq 0 \rightarrow x \# 0)$, $\langle s_n \rangle_n \in x$, $\langle s_n \rangle_n$ defined by $s_n = 0$ if $\neg \exists y \leq n (ay = 0)$, $s_n = 2^{-k}$ if $k = \min_y [ay = 0]$, then $\exists y (ay = 0) \leftrightarrow x \# 0$, $\neg \neg \exists y (ay = 0) \leftrightarrow x \neq 0$, hence by $\forall x (x \neq 0 \rightarrow x \# 0)$, M follows. $\square$

Far more interesting is the continuity theorem of CRA: with the help of M one can show that the continuity of mappings from complete separable metric spaces into separable metric spaces (see e.g. MOSCHOVAKIS [1964], which is written from the viewpoint of classical recursive analysis, but which can be adapted easily to CRA). We have not formulated the most general theorem of this kind here.

In BEESON [1975] (exposition also in TROELSTRA [1973a], §3.9) it is shown that **HA** + ECT₀ is *not* sufficient to derive this continuity theorem. Inspection of the proof of the continuity theorem in CRA shows that continuity holds in this case for reasons quite different from the reasons leading to continuity in the case of choice sequences.

8.3. Markov's principle with choice parameters

Note first of all that $M(\text{LS})$ (i.e. $M(\mathcal{U})$ with $\mathcal{U}$ universe of lawless sequences) is obviously false, for then

$$\forall \alpha \neg \neg \exists x (\alpha x = 0) \wedge \neg \forall \alpha \exists x (\alpha x = 0).$$

This is seen as follows: $\neg \exists x (\alpha x = 0)$ implies the existence of an n such that $\alpha \in n$, $\forall \beta \in n \neg \exists x (\beta x = 0)$ which is obviously false (take a $\beta \in n * \langle 0 \rangle$); and $\forall \alpha \exists x (\alpha x = 0)$ would imply the existence of an e such that $\forall \alpha (\alpha(e(\alpha)) = 0)$, $\forall \alpha \exists x (e(\bar{\alpha}x) \neq 0)$, $\forall nm (en \neq 0 \rightarrow en = e(n * m))$, $\forall a \exists x (e(\bar{a}x) \neq 0)$; but then also $e(\lambda x. 1)$ is defined, and computable from $(\lambda x. 1)y = n$; therefore if we choose $\text{lth}(n) > en \dot{-} 1$, it follows that $(\lambda x. 1)(en \dot{-} 1) = 0$.

For many other notions of choice sequence Markov's principle is suspect as well. Let us consider the following very special form

$$\begin{aligned} M_{PR}^{*-} \quad & \forall \alpha \leq \lambda x. 1 \neg \neg \exists x A(\bar{\alpha}x) \rightarrow \\ & \rightarrow \neg \neg \forall \alpha \leq \lambda x. 1 \exists x A(\bar{\alpha}x) \quad (A \text{ primitive recursive}). \end{aligned}$$

Note that M_{PR}^{*-} is a consequence of $M(\mathcal{U})$ if α ranges over $\mathcal{U}$ and $\mathcal{U}$ is closed under lawlike continuous operations. We have:

PROPOSITION. *Let $\mathbf{H}$ be a theory as described in 6.13, and let $\mathbf{CS}^*$ be similar to $\mathbf{CS}_H$ but with $\forall \alpha \exists x (e(\bar{\alpha}x) \neq 0)$ left out; let $\mathcal{U}$ be the range of the choice variables. Then*

- (i) $M(\mathcal{U}) + \mathbf{CS}^* \vdash \forall \alpha \exists x (e(\bar{\alpha}x) \neq 0)$,
- (ii) in $\mathbf{CS}_H + M_{PR}^{*-} \vdash \neg \mathbf{CT}$, where as before

$$\mathbf{CT} \quad \forall a \exists x \forall y \exists z (Txyz \wedge ay = Uz).$$

PROOF. (i) Any e satisfies (provably in $\mathbf{H}$)

$$\forall b \exists x (e(\bar{b}x) \neq 0), \quad \forall nm (en \neq 0 \rightarrow en = e(n * m)). \quad (1)$$

If $\exists \alpha A\alpha$ is closed, then $\exists \alpha A\alpha \rightarrow \exists a Aa$: apply A2 of 6.13 to $\forall \beta \exists \alpha A\alpha$, then $\exists e \forall \alpha A(e \mid \alpha)$, hence $A(e \mid \lambda^n x. 0)$. Applying this to $\exists \alpha \neg \exists a (\alpha = a)$ yields a contradiction, hence $\forall \alpha \neg \neg \exists a (\alpha = a)$. Then (1) implies

$$\forall \beta \neg \neg \exists x (e(\bar{\beta}x) \neq 0).$$

Now apply $M(\mathcal{U})$ with $\lambda x. (1 \div e(\bar{\beta}x))$ for α , then $\forall \beta \exists x (e(\bar{\beta}x) \neq 0)$.

(ii) Kleene constructed a binary tree with primitive recursive characteristic function which is well-founded w.r.t. recursive sequences but not uniformly bounded (see e.g. KLEENE and VESLEY [1965], Lemma 9.8). So, on assumption of CT, there is a primitive recursive φ such that

$$\forall a \exists x (\varphi(\bar{a}x) \neq 0),$$

$$\forall nm (\varphi n \neq 0 \rightarrow \varphi n = \varphi(n * m)),$$

but $\varphi \notin K_1$. On the other hand, as in the proof of (i) it follows that $\forall \alpha \neg \neg \exists x (\varphi(\bar{\alpha}x) \neq 0)$, and therefore with M_{PR}^{*-} ,

$$\neg \neg \forall \alpha \leq \lambda x. 1 (\varphi(\bar{\alpha}x) \neq 0),$$

but this is obviously false, since $K \subseteq K_1$, but $\varphi \notin K_1$ (K_1 as defined in 6.6(1)), hence $\neg \forall \alpha \exists x (\varphi(\bar{\alpha}x) \neq 0)$. $\square$

Remark. (a) Crucial in the proof of (i) and (ii) is the property $\forall \alpha \neg \neg \exists a (\alpha = a)$; this is *false* for lawless sequences.

(b) The result of 9.5 shows that completeness of **IPC** implies $M_{PR}^{*\neg}$, hence $\neg CT$; here the relations and domains in the definition of validity may contain lawless and choice parameters, as specified in 9.5. Compare also 9.3.

9. Truth-value semantics for intuitionistic logic; validity in all structures

9.1. The principal interpretations of intuitionistic logic with the character of a truth-value semantics considered in the literature are:

(a) Valuations in complete pseudo-Boolean algebras (or pseudo-Boolean valued models, PBM's for short). Detailed treatment in RASIOWA and SIKORSKI [1963].

(b) Topological models (valuations in the algebra of open subsets of a topological space). See e.g. RASIOWA and SIKORSKI [1963]. Applications in SCOTT [1968, 1970], J. R. MOSCHOVAKIS [1973]. Topological models are special cases of PBM's.

(c) Beth models (principal sources BETH [1959], KRIPKE [1965]). Beth models are special cases of topological models.

(d) Kripke models (KRIPKE [1965], FITTING [1969]; applications in SMORYNSKI [1973a]). Kripke models are defined relative to partially ordered sets; if the partially ordered sets are restricted to countable trees, then Kripke models can be transformed by a standard procedure into a Beth model satisfying the same sentences (see KRIPKE [1965]). Kripke models are always special cases of topological models.

Classically established completeness theorems for the various types of semantics mentioned above can be used to obtain interesting results on intuitionistic formal systems — good examples are to be found in SMORYNSKI [1973a]. Via a detour (formalization of the proof of the completeness theorem in a classical system, and conservativeness of classical systems over the corresponding intuitionistic systems w.r.t. Π_2^0 -formulae) many of these results can also be established intuitionistically. The methods are similar in character to the techniques of classical model theory, treated elsewhere in this volume. Therefore we shall refrain from discussing these semantics here, but turn to the notion of (intuitionistic or constructive) validity in all structures instead.

9.2. Validity and completeness

We define “validity in all structures” in complete analogy with the classical case:

DEFINITION. Let $A(P_1, \dots, P_n)$ be a formula of **IPC**, with all its predicate letters contained among $P_1, \dots, P_n$; then we put

$$\text{Val}(A) \equiv_{\text{def}} \forall D \forall P_1^* \dots \forall P_n^* A^D(P_1^*, \dots, P_n^*)$$

where D is a (intuitionistically meaningful) domain, P_i^* a relation over D with the same number of arguments as P_i , $A^D(P_1^*, \dots, P_n^*)$ obtained from A by relativizing quantifiers to D and replacing P_i by P_i^* ($1 \leq i \leq n$).

The following results illustrate the influence of *mathematical* assumptions on the extension of $\{^{\ulcorner}A^{\urcorner} : \text{Val}(A)\}$.

9.3. THEOREM. *Assuming CT, and restricting domains and relations to completely defined ones (i.e. not containing non-lawlike parameters) $\{^{\ulcorner}A^{\urcorner} : \text{Val}(A)\}$ is not r.e. (KREISEL [1970], exposition in VAN DALEN [1973]).*

Remark. In fact, the restriction to completely defined domains and relations can be weakened considerably.

On the other hand, suppose we restrict D to $\mathbb{N}$, and the P_i^* to numerical relations containing a lawless parameter (more precisely, lawless relative to a finitely branching tree), then we obtain completeness for prenex formulae of **IPC**:

9.4. THEOREM. *For A prenex,*

$$\text{Val}(A) \rightarrow \exists x \text{Proof}_{\text{IPC}}(x, ^{\ulcorner}A^{\urcorner})$$

and

$$\neg \exists x \text{Proof}_{\text{IPC}}(x, ^{\ulcorner}A^{\urcorner}) \rightarrow \exists P_1^e, \dots, P_n^e \neg \forall \varepsilon A^{\mathbb{N}}(P_1^e, \dots, P_n^e),$$

where P_i^e is a predicate of natural numbers depending on a lawless parameter ε .

The weak form of Markov's principle for choice sequences, M_{PR}^{*-} plays a role in the following result:

9.5. THEOREM (DYSON and KREISEL [1961], KREISEL [1962], TROELSTRA [1977a], Ch. 7). *Let, in $\text{Val}(A)$, $D = \mathbb{N}$, $P_i^* \subseteq \mathbb{N}^{\tau(i)}$, P_i^* containing, besides lawless parameters, choice parameters α for sequences of 0, 1 which are assumed to satisfy*

$$\forall n \in B \exists \alpha (\alpha \in n),$$

$$\forall \alpha \leq \lambda x.1 \exists x A(\bar{\alpha}x) \rightarrow \exists z \forall \alpha \leq \lambda x.1 \exists x \leq z A(\bar{\alpha}x),$$

where A is quantifier-free and $n \in B \equiv_{\text{def}} \forall x < \text{lth}(n) ((n)_x \leq 1)$, then weak completeness

$$\text{Val}(A) \rightarrow \neg \neg \exists x \text{Proof}_{\text{IPC}}(x, \ulcorner A \urcorner)$$

for all A of IPC is equivalent to M_{PR}^* .

For much more details and a leisurely discussion, see TROELSTRA [1977a, Ch. 7; 1977b].

10. Finite type structures

10.1. The language $L(\text{N-HA}^\omega)$

The collection of finite types $\mathbf{T}$ is defined inductively by

- (i) $0 \in \mathbf{T}$,
- (ii) $\sigma, \tau \in \mathbf{T} \Rightarrow (\sigma)\tau \in \mathbf{T}$.

A model for this type structure is given by specifying a set D_σ for each $\sigma \in \mathbf{T}$; in our examples, $D_0 = \mathbb{N}$, the set of natural numbers; $D_{(\sigma)\tau}$ consists of a set of operations (depending on the model) assigning objects of D_τ to objects of D_σ . We have preferred to use the neutral term “operation” instead of “function” or “mapping” since the use of the latter expressions might suggest to the reader functions which are extensional in the sense of classical set theory, whereas we also wish to consider models where the operations are non-extensional.

$L(\text{N-HA}^\omega)$ contains variables for each type ($x^\sigma, y^\sigma, z^\sigma, u^\sigma, v^\sigma, w^\sigma$; type superscripts are often omitted); equality $=_\sigma$ for all types σ , and constants

$$0 \in 0, \quad S \in (0)0, \quad \Pi_{\sigma, \tau} \in (\sigma)(\tau)\sigma,$$

$$\Sigma_{\rho, \sigma, \tau} \in ((\rho)(\sigma)\tau)((\rho)\sigma)(\rho)\tau,$$

$$R_\sigma \in (\sigma)((0)(\sigma)\sigma)(0)\sigma \quad \text{for all } \rho, \sigma, \tau \in \mathbf{T};$$

we use here as in the sequel $t \in \sigma$ to indicate that t is a term of type σ . Application from type $(\sigma)\tau$ to type σ is also present and simply denoted by juxtaposition; $t_1 \cdots t_n$ abbreviates $(\cdots ((t_1 t_2) t_3) t_4 \cdots) t_n$.

10.2. The theory N-HA^ω

The theory is based on many-sorted intuitionistic predicate logic, the usual axioms for successor, “defining axioms” for Π, Σ, R specified below,

and for equality, besides symmetry, reflexivity and transitivity also substitutivity

$$\begin{aligned}x^\sigma &= y^\sigma \rightarrow z^{(\sigma)\tau} x^\sigma = z^{(\sigma)\tau} y^\sigma, \\x^{(\sigma)\tau} &= y^{(\sigma)\tau} \rightarrow x^{(\sigma)\tau} z^\sigma = y^{(\sigma)\tau} z^\sigma.\end{aligned}$$

We shall frequently omit type superscripts from now on, types are assumed to be coherent. The defining axioms for Π, Σ, R are

$$\Pi xy = x, \quad \Sigma xyz = xz(yz), \quad Rxy0 = x, \quad Rxy(Sz) = y(Rxyz)z.$$

10.3. Models for $\mathbf{N-HA}^\omega$

Detailed information and further references concerning the models discussed here in TROELSTRA [1973a], Ch. 2.

10.3.1. The lawlike operations LO (GÖDEL [1958], called “berechenbare Funktion” there.)

$D_{(\sigma)\tau}$ consists of all lawlike operators assigning elements of D_τ to all elements of D_σ . Relying on the intuitive meaning of lawlike, there are obviously representatives of Π, Σ, R in this model. $t =_\sigma t'$ means: t, t' are *given* to us as the same law ($=_\sigma$ is intensional equality).

10.3.2. The hereditarily recursive operations HRO

We put

$$\begin{aligned}V_0(x) &\equiv_{\text{def}} x = x, \\V_{(\sigma)\tau}(x) &\equiv_{\text{def}} \forall y \in V_\sigma \exists z \in V_\tau (\{x\}(y) \approx z).\end{aligned}$$

We put $D_\sigma = \{(x, \sigma) : x \in V_\sigma\}$ in this model. Application is partial recursive function application

$$(\{x\}, (\sigma)\tau)(y, \sigma) = (\{x\}(y), \tau)$$

and

$$(x, \sigma) = (y, \sigma) \equiv_{\text{def}} x = y.$$

We can show HRO to be a model for $\mathbf{N-HA}^\omega$ if we can find numbers $[0], [S], [\Pi_{\sigma,\tau}], [\Sigma_{\rho,\sigma,\tau}], [R_\sigma]$ such that the defining equations are satisfied, e.g. $([\Pi], (\sigma)\tau)(x, \sigma)(y, \tau) = (x, \sigma)$, which means that we have to find $[\Pi]$ such that $\{[\Pi]\}(x)(y) \approx x$ for $x \in V_\sigma, y \in V_\tau$; we may take $\lambda x \lambda y. x$ for $[\Pi_{\sigma,\tau}]$. Similarly, $[0] = 0$, $[S] = \lambda x. x + 1$, $[\Sigma_{\rho,\sigma,\tau}] = \lambda xyz. \{x\}(z)\{y\}(z)$. The most complicated case is $[R_\sigma]$, which can be found by an application of the recursion theorem (which is redundant in case recursion is already under the basic schemata for recursive functions)

HRO may be viewed as a sort of “recursive approximation” to LO. For LO, intuitively, a choice axiom

$$AC_{\sigma, \tau} \quad \forall x^\sigma \exists y^\tau A(x, y) \rightarrow \exists z^{(\sigma)\tau} \forall x^\sigma A(x, zx)$$

is a consequence of the meaning of the quantifier combination $\forall x \exists y$ (but indeed only if we permit the most general kind of non-extensional operations defined on D_σ as elements of $D_{(\sigma)\tau}$).

For HRO, consistency of $AC_{\sigma, \tau}$ is provable relative **HA** — in fact, $AC_{\sigma, \tau}$ is derivable for HRO in **HA** + ECT_0 .

10.3.3. The hereditarily effective operations HEO

An extensional model is obtained by defining simultaneously for each $\sigma \in \mathbf{T}$ equivalence relations I_σ and domains W_σ :

$$I_0(x, y) \equiv x = y, \quad W_0(x) \equiv x = x,$$

$$I_{(\sigma)\tau}(x, y) \equiv W_{(\sigma)\tau}(x) \wedge W_{(\sigma)\tau}(y) \wedge \forall z \in W_\sigma (\{x\}(z) \approx \{y\}(z)),$$

$$W_{(\sigma)\tau}(x) \equiv \forall y \in W_\sigma (\exists z \in W_\tau (\{x\}(y) \approx z) \wedge \forall y' \in W_\sigma (I_\sigma(y, y') \rightarrow \\ \rightarrow I_\tau(\{x\}(y), \{x\}(y')))).$$

D_σ for this model now consists of pairs (x, σ) with $x \in W_\sigma$. Application is defined as before, and

$$(x, \sigma) =_\sigma (y, \sigma) \equiv_{\text{def}} I_\sigma(x, y).$$

Interpretations of $R_\sigma, \Pi_{\sigma, \tau}, \Sigma_{\rho, \sigma, \tau}, 0, S$ are constructed as for HRO.

10.3.4. The intensional continuous functionals ICF($\mathcal{U}$)

This an analogue to HRO, but now based on continuous function application instead of partial-recursive function application. We define

$$V_0^1(x) \equiv x = x, \quad V_1^1(\alpha) \equiv \alpha = \alpha,$$

$$V_{(\sigma)0}^1(\alpha) \equiv \forall \gamma \in V_\sigma^1 \exists x (\alpha(\gamma) \approx x) \quad (\sigma \neq 0),$$

where

$$\alpha(\gamma) \approx x \equiv_{\text{def}} \alpha(\tilde{\gamma} \min_z [\alpha(\tilde{\gamma}z) \neq 0]) = x \dot{+} 1,$$

$$V_{(0)\sigma}^1(\alpha) \equiv \forall x \exists \gamma \in V_\sigma^1 (\alpha \mid \lambda z. x \approx \gamma) \quad (\sigma \neq 0)$$

and for $\sigma, \tau \neq 0$,

$$V_{(\sigma)\tau}^1(\alpha) \equiv \forall \beta \in V_\sigma \exists \gamma \in V_\tau (\alpha \mid \beta \approx \gamma),$$

where $(\alpha \mid \beta) \approx \gamma \equiv \forall x (\lambda n. \alpha(\hat{x} * n)(\beta) \approx \gamma x)$. The objects of type 0 are the pairs $(x, 0)$, objects of type $\sigma, \sigma \neq 0$ are the pairs (α, σ) with $\alpha \in V_\sigma^1$.

Equality is interpreted as

$$(\alpha, \sigma) =_{\sigma} (\beta, \sigma) \equiv_{\text{def}} \forall x (\alpha x = \beta x),$$

and application by $(\sigma, \tau \neq 0)$

$$(\alpha, 1)(x, 0) = (\alpha x, 0), \quad (\alpha, (0)\sigma)(x, 0) = (\alpha \mid \lambda z. x, \sigma),$$

$$(\alpha, (\sigma)0)(\beta, \sigma) = (\alpha(\beta), 0), \quad (\alpha, (\sigma)\tau)(\beta, \sigma) = (\alpha \mid \beta, \tau).$$

From the formalized theory of recursive functionals one then obtains interpretations of $R_{\sigma}, \Pi_{\sigma, \tau}, \Sigma_{\rho, \sigma, \tau}, S, 0$.

The properties of $\text{ICF}(\mathcal{U})$ depend on $\mathcal{U}$ of course: if $\mathcal{U}$ consists of the recursive functions, type 2 functionals in ICF are not necessarily uniformly continuous on *bounded* subsets of functions; if $\mathcal{U}$ satisfies the fan theorem, uniform continuity holds.

10.3.5. The countable or extensional continuous functionals $\text{ECF}(\mathcal{U})$

This is the extensional analogue of $\text{ICP}(\mathcal{U})$, related to $\text{ECF}(\mathcal{U})$ in the same manner as HEO to HRO (KLEENE [1959], KREISEL [1959]).

Other models of $\mathbf{N-HA}^{\omega}$ which we shall not discuss here are (a) recursive objects of higher type, (b) term models, (c) hereditarily majorizable functionals (HOWARD [1973]), (d) the hybrid $\text{ICF}'(\mathcal{U})$ obtained by restricting $\text{ICF}(\mathcal{U})$ to its recursive elements.

10.4. The uses of non-extensional models

10.4.1. As has been remarked above, HRO may be regarded as a recursive approximation to the more “fundamental” model LO. As an object of study, HRO is more manageable than LO because it is defined in terms of well-known notions. The example of HRO shows that there is nothing paradoxical or incoherent in the concept of a decidable non-extensional notion of equality. In fact, HRO is not only a model of $\mathbf{N-HA}^{\omega}$, but also of the theory $\mathbf{I-HA}^{\omega}$, obtained from $\mathbf{N-HA}^{\omega}$ by addition of the constants E_{σ} satisfying

$$E_{\sigma}xy \leq 1, \quad E_{\sigma}xy = 0 \leftrightarrow x =_{\sigma} y.$$

$\mathbf{I-HA}^{\omega}$ may be viewed as a theory of finite type objects with strict (intensional) equality: two objects are intensionally equal (identical) if they are given to us as the same object; and HRO shows that $\mathbf{I-HA}^{\omega}$ has a simple model. It has been argued that the introduction of intensional equality in the language depends on a confusion between “use” and “mention”. But even if one assumes the objects of a type structure to be

rules given by a *linguistic* representation, there is still the distinction between the rules as mathematical objects and their names (where it is irrelevant that the names may be such that they contain complete descriptions of the rules). HRO illustrates the point — all its objects may be conceived as rules, but they do not all have names (= closed terms) in $\mathbf{N-HA}^\omega$ or $\mathbf{I-HA}^\omega$. $\mathbf{I-HA}^\omega$ can be interpreted as a theory of rules-as-objects.

Note that in the description of models such as HRO, HEO, ICF we have to make essential use of logic: the definition of V_σ for example is of increasing logical complexity with increasing complexity of σ .

10.4.2. Technical uses

(a) One simple application of HRO is immediate: $\mathbf{I-HA}^\omega$ is a conservative extension of $\mathbf{HA}$, since interpretation of the quantifiers in $\mathbf{I-HA}^\omega$ as ranging over the elements of HRO leaves formulae of $\mathbf{HA}$ (essentially) unchanged. (Similarly, $\mathbf{E-HA}^\omega$ where equality between higher type objects is defined by $x^{(\sigma)\tau} = y^{(\sigma)\tau} \equiv \forall z^\sigma (xz = yz)$ is a conservative extension of $\mathbf{HA}$, as may be seen with the help of HEO.)

(b) The preceding application still referred explicitly to non-extensional equality in the statement of its result. More convincing are results not referring to non-extensional equality; such results can be obtained by combination with functional interpretations (modified realizability, Dialectica interpretation). One such example is given in 11.7.3; for other examples, see TROELSTRA [1975], §3 and the references given there.

The crucial fact on which these applications rest is that schemata such as $\mathbf{CT}_0$, $\mathbf{CONT}_0$ have a functional interpretation only if we permit non-extensional models for the finite type structure.

10.5. Bar-recursive functionals

The so-called bar-recursive functionals have attracted much attention ever since they were introduced in SPECTOR [1962]. For a survey, see KREISEL [1968].

Here our principal reason for including them is to show how to obtain a Dialectica interpretation for (a part of) classical analysis (cf. 11.8); this in turn will be used in discussing the constructivization of classical theorems in Section 12. We cannot show all the steps of the way, but we intend to give the reader an idea of the route to be followed; the details may be completed with the help of easily accessible sources.

Let us extend $\mathbf{N-HA}^\omega$ by addition of types σ^U for finite sequences of

objects of type σ , with corresponding variables, and some obvious axioms stating properties of the length function, concatenation etc. The result is a definitional extension, since we can identify the objects of type $\sigma^\cup$ with special sequences of type $(0)\sigma$, e.g. as follows.

Code natural numbers into higher types, putting $n_0 = n$, $n_{(\sigma)\tau} = \Pi_{\sigma,\tau} n_\tau$; then n_σ codes n in type σ . We then code $\langle x_\sigma^0, \dots, x_{\sigma^{u-1}}^\sigma \rangle$ as $z^{(0)\sigma}$ with

$$\begin{aligned} z^{(0)\sigma}(0) &= u_\sigma, & z^{(0)\sigma}(i+1) &= x_i^\sigma \quad \text{for } i < u, \\ z^{(0)\sigma}i &= 0_\sigma \quad \text{for } i > u. \end{aligned}$$

Now let c be a variable of type $\sigma^\cup$, ranging over finite sequences of objects of type σ , and let us adopt notations similar to those for finite sequences of natural numbers, e.g. $c_1 * c_2$, $\hat{u} = \langle u \rangle$ ($u \in \sigma$), $\text{lth}(c)$.

Let $[c]$ denote a sequence of type $(0)\sigma$ where if $c = \langle u_0, \dots, u_{x-1} \rangle$, $[c](i) = u_i$ for $i < x$ and $[c](i) = 0_\sigma$ for $i \geq x$.

We note, for reference below, that we can define a λ -abstraction operator of type σ by induction on the construction of terms by

$$\begin{aligned} \lambda x^\sigma. x^\sigma &= \Sigma_{\sigma, (\sigma)\sigma, \sigma} \Pi_{\sigma, (\sigma)\sigma} \Pi_{\sigma, \sigma}, \\ \lambda x^\sigma. t^\tau &= \Pi_{\tau, \sigma} t^\tau \quad \text{for } x \text{ not occurring in } t, \\ \lambda x^\sigma. t_1 t_2 &= \Sigma(\lambda x^\sigma. t_1)(\lambda x^\sigma. t_2). \end{aligned}$$

The bar-recursion constants B_σ^τ (rank σ , level τ) then should satisfy the defining axioms

$$\text{BR}_\sigma \quad \left\{ \begin{array}{l} y[c] < \text{lth}(c) \rightarrow B_\sigma^\tau y z u c = z c, \\ y[c] \geq \text{lth}(c) \rightarrow B_\sigma^\tau y z u c = u(\lambda v. B_\sigma^\tau y z u(c * \hat{v})), \\ \text{with } z \in (\sigma^\cup)\tau, \quad y \in ((0)\sigma)0, \quad u \in ((\sigma)\tau)(\sigma^\cup)\tau. \end{array} \right.$$

To see (at least classically) that BR_σ defines a functional, y must be assumed to be continuous, i.e. yz depending on an initial segment of z only; then for $y[c] < \text{lth}(c)$, $B_\sigma^\tau y z u c$ is determined directly, and for $y[c] \geq \text{lth}(c)$ the computation of $B_\sigma^\tau y z u c$ is thrown back on the computation of $B_\sigma^\tau y z u(c * \hat{v})$ for all v of type σ . If the set of c such that $y[c] \geq \text{lth}(c)$ constitutes a well-founded tree (classically a consequence of continuity) the computation is finally reduced to cases with $y[c] < \text{lth}(c)$.

We shall often simply write B_σ for B_σ^τ . $\text{BR} = \bigcup_{\sigma \in \mathbf{T}} \text{BR}_\sigma$.

10.5.1. DEFINITION. BI_σ denotes the schema

$$(1) \wedge (2) \wedge (3) \wedge (4) \rightarrow Q(\langle \quad \rangle),$$

where

- (1) $\forall z^{(0)\sigma} \exists x P(\bar{z}x),$
- (2) $\forall c c'(Pc \rightarrow P(c * c')),$
- (3) $\forall c (Pc \rightarrow Qc),$
- (4) $\forall c (\forall u Q(c * \hat{u}) \rightarrow Qc).$

(BI therefore corresponds to BI_0 .)

10.5.2. THEOREM. $ECF(\mathcal{U})$ for a universe $\mathcal{U}$ satisfying BI_0 is a model for BR_0 , BR_1 , i.e. contains elements $([B_0^i], \sigma')$, $([B_1^i], \sigma'')$ for appropriate σ' , σ'' which satisfy the equations for bar-recursion of types 0 and 1.

PROOF (outline). One can show either directly, or with the help of a recursion theorem analogue (TROELSTRA [1973a] 1.9.16, 2.9.10) the existence of constant (primitive recursive) functions ε_0 , ε_1 satisfying the equations for BR_0 , BR_1 , but with $\approx$ instead of $=$; to show that $\varepsilon_i \in W_i^1$, where i^* is the type of B_i^i for $i = 0, 1$ (which would justify the choice of ε_i for $[B_i^i]$) we need BI_0 , BI_1 respectively. As shown in HOWARD and KREISEL [1966], Theorem 7B, BI_1 can be obtained from BI_0 ; the instances of the "strong axiom of continuity" needed for the proof hold trivially in the special cases of BI_1 needed here. $\square$

11. The Dialectica interpretation

11.1. Some conventions and notations

We shall use $\mathfrak{x}, \mathfrak{y}, \mathfrak{z}, u, \mathfrak{X}, \mathfrak{Y}, \dots$ for sequences of variables of finite type, $\mathfrak{s}, \mathfrak{t}, \mathfrak{S}, \mathfrak{T}$ for sequences of terms of finite type. When $\mathfrak{s} = (s_1, \dots, s_n)$, $s_i \in (\tau_1) \cdots (\tau_m)\sigma_i$, $\mathfrak{t} = (t_1, \dots, t_m)$, $t_i \in \tau_i$, then

$$\mathfrak{st} = (s_1 t_1 \cdots t_m, \dots, s_n t_1 \cdots t_m).$$

For $\mathfrak{t}$ empty, $\mathfrak{st} = \mathfrak{s}$; for $\mathfrak{s}$ empty, $\mathfrak{st}$ is empty. $\forall \mathfrak{s}$ abbreviates $\forall s_1 \cdots \forall s_n$, $\forall \mathfrak{st}$ abbreviates $\forall \mathfrak{s} \forall \mathfrak{t}$; similarly for $\exists \mathfrak{s}$ and $\exists \mathfrak{st}$.

11.2. Definition of the translation

To each formula $A \mathfrak{z}$ of the language $\mathbf{N} - \mathbf{HA}^\omega$ we associate another formula $A^D \equiv \exists \mathfrak{x} \forall \mathfrak{y} A_D(\mathfrak{x}, \mathfrak{y}, \mathfrak{z})$, A_D quantifier-free, as follows. The types of $\mathfrak{x}, \mathfrak{y}$ depend on the logical structure of A only; all the free variables of A^D are contained among the free variables of A .

d(i) If A is prime, then $A^D \equiv A_D \equiv A$.

For the other clauses, let $A^D \equiv \exists \mathfrak{x} \forall \mathfrak{y} A_D(\mathfrak{x}, \mathfrak{y})$, $B^D \equiv \exists u \forall v B_D(u, v)$.

$$d(ii) (A \wedge B)^D \equiv \exists x u \forall \eta v [A \wedge B]_D \equiv \exists x u \forall \eta v [A_D(x, \eta) \wedge B_D(u, v)].$$

$$d(iii) (A \vee B)^D \equiv \exists z {}^0 x u \forall \eta v [A \vee B]_D \equiv \\ \equiv \exists z {}^0 x u \forall \eta v [(z = 0 \rightarrow A_D(x, \eta)) \wedge (z \neq 0 \rightarrow B_D(u, v))].$$

$$d(iv) (\exists z A z)^D \equiv \exists z x \forall \eta (\exists z A z)_D \equiv \exists z x \forall \eta A_D(x, \eta, z).$$

$$d(v) (\forall z A z)^D \equiv \exists x \forall z \eta (\forall z A z)_D \equiv \exists x \forall z \eta A_D(x, z, \eta).$$

d(vi) We split the construction of $(A \rightarrow B)^D$ into a number of smaller steps:

$$(A \rightarrow B)^D \equiv [\exists x \forall \eta A_D \rightarrow \exists u \forall v B_D]^D \equiv \quad (a)$$

$$\equiv [\forall x (\forall \eta A_D \rightarrow \exists u \forall v B_D)]^D \equiv \quad (b)$$

$$\equiv [\forall x \exists u (\forall \eta A_D \rightarrow \forall v B_D)]^D \equiv \quad (c)$$

$$\equiv [\forall x \exists u \forall v (\forall \eta A_D \rightarrow B_D)]^D \equiv \quad (d)$$

$$\equiv [\forall x \exists u \forall v \exists \eta (A_D \rightarrow B_D)]^D \equiv \quad (e)$$

$$\equiv [\exists \eta \forall x \forall v (A_D(x, \eta, v) \rightarrow B_D(\eta, x, v))]. \quad (f)$$

$$(A \rightarrow B)_D \equiv A_D(x, \eta, v) \rightarrow B_D(\eta, x, v).$$

11.2.1. Note: with classical logic and AC, $A^D \equiv A$ for all A , since (even intuitionistically) $A^D \equiv A$ for prime A , $(A \wedge B)^D \leftrightarrow (A^D \wedge B^D)$, $(A \vee B)^D \leftrightarrow A^D \vee B^D$, $(\exists z A)^D \leftrightarrow \exists z A^D$; with AC $(\forall z A)^D \leftrightarrow \forall z A^D$, and with AC and classical logic $(A \rightarrow B)^D \leftrightarrow (A^D \rightarrow B^D)$ as shown by inspection of the steps (a)–(f). This result will be refined below in 11.5–11.6.

11.2.2. Note also that

(i) if $A \equiv \exists x \forall \eta B$, B quantifier-free, then $A^D \equiv A$;

(ii) for quantifier-free B , $(\neg\neg\exists x B)^D \equiv (\neg\forall x \neg B)^D \equiv \exists x \neg\neg B$; for the extensions and subsystems of $\mathbf{N-HA}^\omega$ which interest us quantifier-free formulae are decidable, hence $(\neg\neg\exists x B)^D \leftrightarrow \exists x B$ in such cases.

11.2.3. The motivation for the definition of $(A \rightarrow B)^D$ may be based on the following two principles: (a) to establish $\exists x A x \rightarrow \exists y B y$, produce a functional Y computing the y from the x , i.e. $A x \rightarrow B(Yx)$; (b) to establish $\forall x A x \rightarrow \forall y B y$, read it as $\exists y \neg B y \rightarrow \exists x \neg A x$, and apply (a); with another contraposition $A(Xy) \rightarrow B y$.

11.3. DEFINITION. Let $\mathbf{WE-HA}^\omega$ be the system similar to $\mathbf{N-HA}^\omega$, but with only $=_0$ as a primitive, $=_\sigma$ being defined hereditarily by

$$x^{(\sigma)\tau} = y^{(\sigma)\tau} \equiv_{\text{def}} \forall x^\sigma (x z = y z)$$

and with a rule of extensionality

$$\vdash P \rightarrow tx_1 \cdots x_n = sx_1 \cdots x_n, \quad \vdash At \Rightarrow \vdash P \rightarrow As,$$

where $x_1, \dots, x_n$ are such that $tx_1 \cdots x_n, sx_1 \cdots x_n$ are numerical terms, P a propositional combination of prime formulae (i.e. equations between terms of type 0).

qf-WE-HA $^\omega$, qf-I-HA $^\omega$ are the quantifier-free parts of WE-HA $^\omega$, I-HA $^\omega$, with induction replaced by the rule (for quantifier-free A)

$$\vdash A0, \quad \vdash Ax \rightarrow A(Sx) \Rightarrow \vdash Ax.$$

11.4.1. SOUNDNESS THEOREM. *For $\mathbf{H} = \mathbf{WE-HA}^\omega$ or $\mathbf{I-HA}^\omega$: if $\mathbf{H} \vdash A$, then for a suitable sequence of terms t ,*

$$\text{qf-}\mathbf{H} \vdash \forall \eta A_D(t, \eta).$$

For most applications, the following weaker corollary suffices:

11.4.2. COROLLARY. *For $\mathbf{H} = \mathbf{WE-HA}^\omega$, $\mathbf{I-HA}^\omega$: if $\mathbf{H} \vdash A$, then $\mathbf{H} \vdash \forall \eta A_D(t, \eta)$ for a suitable sequence of terms t .*

PROOF. The proof is by induction on the length of derivations in $\mathbf{H}$. Most cases are routine, except the verification for $A \rightarrow A \wedge A$ and induction. If we are only interested in establishing the corollary, induction becomes straightforward too. So let us restrict attention to $A \rightarrow A \wedge A$. Assume $A^D = \exists x \forall \eta A_D$;

$$\begin{aligned} [A \rightarrow A \wedge A]^D &= \\ &= \exists \mathcal{Y} \mathcal{X} \mathcal{X}' \forall x \eta' \eta'' [A_D(x, \mathcal{Y} x \eta' \eta'') \rightarrow A_D(\mathcal{X} x, \eta') \wedge A_D(\mathcal{X}' x, \eta'')]. \end{aligned}$$

To find a solution, at a first try take $\lambda x. x$ for $\mathcal{X}'$ and $\mathcal{X}$, and look for a $\mathcal{Y}$ with the following properties: if $A_D(x, \eta')$ is *false*, $A_D(x, \mathcal{Y} x \eta' \eta'')$ must be false, which can be achieved taking $\mathcal{Y} x \eta' \eta'' = \eta'$ in this case; if $A_D(x, \eta')$ is true, we want $\mathcal{Y} x \eta' \eta'' = \eta''$. Since the prime formulae in I-HA $^\omega$ and WE-HA $^\omega$ are decidable, and equality functionals are available, we can construct for each quantifier-free $B \exists$ a term T_B such that $\vdash T_B \exists = 0 \leftrightarrow B \exists$; thus we may take for $\mathcal{Y}$ the term $\mathfrak{T}$ defined by

$$\mathfrak{T} x \eta' \eta'' = \begin{cases} \eta' & \text{if } T_{A_D} x \eta' \neq 0, \\ \eta'' & \text{if } T_{A_D} x \eta' = 0. \quad \square \end{cases}$$

The use of the decidability of prime formulae is *essential* here, as shown by an example due to W.A. Howard (cf. e.g. TROELSTRA [1973a], 2.7.8,

3.5.6): all functionals of $\mathbf{N} - \mathbf{HA}^\omega$ are continuous, but the interpretation of $\forall y^\sigma \neg \forall u^0 \neg (u = 0 \leftrightarrow y^\sigma = z^\sigma)$ by a continuous functional would imply $\neg \neg y^\sigma = z^\sigma \vee \neg y^\sigma = z^\sigma$.

11.5. LEMMA. *Let IP'_0, M' be the schemata*

$$\text{IP}'_0 \quad (\forall \mathbf{x} A \mathbf{x} \rightarrow \exists y B y) \rightarrow \exists y (\forall \mathbf{x} A \mathbf{x} \rightarrow B y),$$

$$\text{M}' \quad \neg \neg \exists \mathbf{x} A \mathbf{x} \rightarrow \exists \mathbf{x} A \mathbf{x}$$

(A quantifier-free, y not free in A).

(i) For $\mathbf{H} = \mathbf{I} - \mathbf{HA}^\omega$, $\mathbf{WE} - \mathbf{HA}^\omega$, F an instance of IP'_0, M' , or AC , $F^D = \exists \eta \forall \mathbf{x} F_D(\mathbf{x}, \eta)$, there is a sequence $\mathbf{t}$ such that $\mathbf{H} \vdash \forall \mathbf{x} F_D(\mathbf{t}, \mathbf{x})$.

(ii) $\mathbf{H} + \text{IP}'_0 + \text{M}' + \text{AC} \vdash A \leftrightarrow A^D$ for all A .

PROOF. (i) is straightforward. (ii) is proved by induction on the complexity of A . The only case requiring some attention occurs when proving $(A \rightarrow B) \leftrightarrow (A \rightarrow B)^D$ on assumption of $A \leftrightarrow A^D, B \leftrightarrow B^D$. We refer to the formulae between brackets in the definition of $[A \rightarrow B]^D$ as (a), (b), ..., (f) respectively. The transition from $A \rightarrow B$ to (a) is permitted by the induction hypothesis, the transition from (a) to (b) by intuitionistic logic, the transition from (b) to (c) requires IP'_0 , (c) to (d) is permitted by intuitionistic logic again, and the transition from (d) to (e) requires M' , since

$$\begin{aligned} (\forall \eta A_D \rightarrow B_D) &\leftrightarrow B_D \vee (\neg B_D \wedge \neg \forall \eta A_D) \leftrightarrow \\ &\leftrightarrow B_D \vee (\neg B_D \wedge \neg \neg \exists \eta \neg A_D) \leftrightarrow \\ &\leftrightarrow (\text{with help of } \text{M}') B_D \vee (\neg B_D \wedge \exists \eta \neg A_D) \leftrightarrow \\ &\leftrightarrow \exists \eta (B_D \vee (\neg B_D \wedge \neg A_D)) \leftrightarrow \exists \eta (A_D \rightarrow B_D). \end{aligned}$$

The transition from (e) to (f) is justified by AC . $\square$

11.6. CHARACTERIZATION THEOREM. *For $\mathbf{H} = \mathbf{I} - \mathbf{HA}^\omega, \mathbf{WE} - \mathbf{HA}^\omega$:*

(i) $\mathbf{H} + \text{M}^\omega + \text{IP}'_0 + \text{AC} \vdash A \leftrightarrow A^D$,

(ii) $\mathbf{H} + \text{M}^\omega + \text{IP}'_0 + \text{AC} \vdash A \leftrightarrow \mathbf{H} \vdash A^D$.

Here $\text{M}^\omega, \text{IP}'_0$ are the schemata

$$\text{M}^\omega \quad \forall \mathbf{x} (A \vee \neg A) \wedge \neg \neg \exists \mathbf{x} A \rightarrow \exists \mathbf{x} A,$$

$$\text{IP}'_0 \quad \forall \mathbf{x} (A \vee \neg A) \wedge (\forall \mathbf{x} A \rightarrow \exists \eta B) \rightarrow \exists \eta (\forall \mathbf{x} A \rightarrow B)$$

PROOF. (i) and (ii) hold with IP'_0, M' instead of IP'_0, M'' . On the one hand, in $\mathbf{WE} - \mathbf{HA}^\omega$, $\mathbf{I} - \mathbf{HA}^\omega$ quantifier-free formulae are provably decidable (for $\mathbf{WE} - \mathbf{HA}^\omega$ since $\forall x^0 y^0 (x = y \vee x \neq y)$ is a theorem of $\mathbf{HA}$, and for $\mathbf{I} - \mathbf{HA}^\omega$ because of this and the presence of E_σ (cf. 10.4.1)), so IP'_0, M' are consequences of M'' , IP'_0 . On the other hand, IP'_0, M'' are derivable from IP'_0, M', AC since by AC

$$\forall \mathbf{x} (A \vee \neg A) \leftrightarrow \exists Z \forall \mathbf{x} ((Z\mathbf{x} = 0 \rightarrow A) \wedge (Z\mathbf{x} \neq 0 \rightarrow \neg A))$$

and thus, replacing A by $Z\mathbf{x} = 0$, M'' and IP'_0 reduce to M', IP'_0 . $\square$

11.7. Applications of the Dialectica interpretation

11.7.1. Foundational applications

The Dialectica interpretation and translation were introduced in GÖDEL [1958]. The original aim was to prove a consistency proof for intuitionistic arithmetic and hence (via the negative translation, see 3.8–3.10) for classical arithmetic, by elimination of logical operators in favour of higher type objects; the notion of a lawlike (constructive) operation of higher type (LO in 10.3) was regarded as intuitively clear and a legitimate extension of finitistic concepts.

TAIT [1967] supplemented this by a proof that every closed term of type 0 in Gödel's calculus (corresponding to our qf- $\mathbf{WE} - \mathbf{HA}^\omega$ or to qf- $\mathbf{I} - \mathbf{HA}^\omega$) could be evaluated, yielding a number as value; but in his proof he needed induction over arithmetically defined predicates of unbounded complexity. In HOWARD [1970], and HINATA [1967] it was shown how to replace this by an ordinal assignment of ordinals $< \varepsilon_0$ to closed terms and quantifier-free ε_0 -induction — thus ultimately achieving the same proof-theoretic reduction as in the Gentzen consistency proof for arithmetic.

As a consequence it remains debatable whether a real reduction has been achieved, depending on one's view of what is intuitively evident. It is worth noting, however, that for systems such as $\mathbf{WE} - \mathbf{HA}^\omega$, $\mathbf{I} - \mathbf{HA}^\omega$ the interpretation shows how logical complexity can be “absorbed” by the complexity due to higher type objects.

11.7.2. Technical application: Markov's rule

One of the best-known and most useful applications of the Dialectica translation is to establish closure under Markov's rule:

$$\text{MR} \quad \vdash \forall x^\sigma (A \vee \neg A), \quad \vdash \neg \neg \exists x^\sigma A \Rightarrow \vdash \exists x^\sigma A$$

for intuitionistic formal systems (see 11.9.(i)). For classical systems $\mathbf{H}^c$

which are conservative over the corresponding intuitionistic system $\mathbf{H}$ w.r.t. negative formulae (such as $\mathbf{HA}$, cf. 3.8–3.10) closure under MR implies that $\mathbf{H}^c$ is conservative over $\mathbf{H}$ w.r.t. Π_2^0 -sentences

$$\mathbf{H}^c \vdash \neg \neg \exists x^0 A \Leftrightarrow \mathbf{H}^c \vdash \neg \forall x^0 \neg A \Leftrightarrow \mathbf{H} \vdash \neg \forall x^0 \neg A \Rightarrow \mathbf{H} \vdash \exists x^0 A.$$

As noted in 9.1, this can be used to justify intuitionistically metamathematical results obtained via classical reasoning on Kripke models. Other derived rules are given in 11.9 below.

11.7.3. Technical application: conservative extension results with the help of non-extensional models

We use a non-extensional model for $\mathbf{I} - \mathbf{HA}^\omega$, namely HRO, to show that $\mathbf{HA} + \mathbf{M} + \mathbf{IP}_0 + \mathbf{CT}_0$ is conservative w.r.t. prenex formulae of $\mathbf{HA}$. Let e.g. $A \equiv \forall x_1 \exists y_1 \forall x_2 B(x_1, y_1, x_2, y_2)$, B quantifier-free, $\mathbf{HA} + \mathbf{M} + \mathbf{IP}_0 + \mathbf{CT}_0 \vdash A$.

We observe that $(\mathbf{CT}_0)^D$ holds in HRO, that is to say, for any instance F of $\mathbf{CT}_0$ $[F^D]_{\text{HRO}}$ is provable in $\mathbf{HA}$. Combining this with the Soundness Theorem (11.4.1) we have $\mathbf{HA} \vdash [A^D]_{\text{HRO}}$; and since $\mathbf{HA} \vdash [A^D]_{\text{HRO}} \rightarrow A$ for prenex A , $\mathbf{HA} \vdash A$.

11.7.4. Constructivization of classical theorems and proofs (See Section 12.)

In preparation for this application, we discuss in 11.8 the extension of the Dialectica interpretation to analysis.

11.8. Extensions to analysis

We now extend $\mathbf{WE} - \mathbf{HA}^\omega$ to a system $\mathbf{BR}_\sigma$ adding the rule $\mathbf{BR}_\sigma$. From HOWARD [1968] for example, we can extract the following extension of the Soundness Theorem:

11.8.1. THEOREM.

$$\mathbf{BR}_\sigma + \mathbf{AC} + \mathbf{BI}_\sigma + \mathbf{M}^\omega + \mathbf{IP}_0^\omega \vdash A \Leftrightarrow \mathbf{BR}_\sigma \vdash A^D.$$

($\mathbf{BI}_\sigma$ defined as in 10.5.)

11.8.2. DEFINITION. Δ_1^1 -comprehension (Δ_1^1 -CA) is the following comprehension schema:

$$\begin{aligned} \Delta_1^1\text{-CA} \quad & \forall y [\forall \alpha \exists x A(\alpha, x, y) \leftrightarrow \exists \beta \forall z B(\beta, z, y)] \rightarrow \\ & \rightarrow \exists \gamma \forall y [\gamma y = 0 \leftrightarrow \forall \alpha \exists x A(\alpha, x, y)] \end{aligned}$$

(A, B quantifier-free). Essentially- Δ_1^1 -comprehension (ess. Δ_1^1 -CA) is formulated similarly, but with $\forall \alpha \exists x$ replaced by a string $\forall \alpha_1 \exists x_1 \forall \alpha_2 \exists x_2 \cdots \forall \alpha_n \exists x_n$ and $\forall \beta \exists z$ by $\exists \beta_1 \forall z_1 \cdots \exists \beta_m \forall z_m$. In Δ_1^1 -CA and ess. Δ_1^1 -CA parameters may be present.

Note that in the presence of $\forall$ -AC₀₁ (AC₀₁ restricted to purely universal formulae) Δ_1^1 -CA is equivalent to ess. Δ_1^1 -CA.

11.8.3. LEMMA. $\forall$ -CA₀₁ *implies* Δ_1^1 -CA *classically*.

PROOF. Classically, with

$$V \equiv \forall y [\forall \alpha \exists x A(\alpha, x, y) \leftrightarrow \exists \beta \forall z B(\beta, z, y)]$$

(A, B quantifier-free) we have

$$V \rightarrow \forall y \exists u [u = 0 \leftrightarrow \forall \alpha \exists x A(\alpha, x, y)]$$

or equivalently

$$V \rightarrow \forall y \exists u [(u \neq 0 \rightarrow \exists \alpha \forall x \neg A(\alpha, x, y)) \wedge (u = 0 \rightarrow \exists \beta \forall z B(\beta, z, y))]$$

hence

$$V \rightarrow \forall y \exists u \exists \alpha \beta \forall xz [(u \neq 0 \rightarrow \neg A(\alpha, x, y)) \wedge (u = 0 \rightarrow B(\beta, z, y))]$$

etc. $\square$

11.8.4. THEOREM. *Let F be an instance of $\forall$ -AC₀₁. Then if F' is the negative Gödel translation of F (cf. 3.8), $\mathbf{BR}_1 \vdash (F')^D$.*

PROOF. See HOWARD [1968]. $\square$

11.8.5. COROLLARY. $\mathbf{EL}^c + \text{ess. } \Delta_1^1\text{-CA} \vdash A \Rightarrow \mathbf{BR}_1 \vdash (A')^D$.

Note that ess. Δ_1^1 -CA includes arithmetical and hyperarithmetical comprehension (as is easily seen by quantifier manipulations).

11.8.6. REMARK. HOWARD [1968] in fact establishes much more than is stated in the theorem; full classical analysis can be Dialectica interpreted (via the negative translation) in $\mathbf{BR} = \bigcup_{\sigma \in \mathbf{T}} \mathbf{BR}_\sigma$. Howard's treatment is an improvement of SPECTOR [1962].

11.9. THEOREM (derived rules as applications of the Dialectica translation).

(i) In $\mathbf{WE} - \mathbf{HA}^\omega$ or $\mathbf{BR}_\sigma$ MR holds

MR $\vdash \forall x^\sigma (A \vee \neg A), \quad \vdash \neg \neg \exists x^\sigma A \Rightarrow \vdash \exists x^\sigma A.$

(ii) Let A be prenex, B quantifier-free. Then

$$\mathbf{HA}^c \vdash A \rightarrow \forall u \exists v B(u, v) \Rightarrow \mathbf{HA} \vdash A \rightarrow \forall u \exists v B(u, v).$$

(iii) Let $C = A \rightarrow \forall u \exists v B(u, v)$ be as in (ii), but with numerical $\forall$ in A only; then

$$\mathbf{EL}^c + \text{ess. } \Delta_1^1\text{-CA} \vdash C \Rightarrow \mathbf{EL} + \mathbf{BI}_0 + \mathbf{AC}_{01} \vdash C.$$

(iv) If A is purely universal, then the conclusion of (iii) can be reinforced to $\mathbf{IDB}_1 \vdash C$ ($\mathbf{IDB}_1$ defined as in 6.20).

PROOF. (i) Let A contain an additional parameter y^τ besides x^σ . Assume $\vdash \forall x^\sigma (A \vee \neg A), \vdash \neg \neg \exists x^\sigma A$, and let us assume the choice rule

$$\mathbf{ACR} \quad \vdash \forall x^\sigma \exists y^\tau A(x, y) \Rightarrow \vdash \forall x^\sigma A(x, tx)$$

to be established for $\mathbf{H}$ (this can be done via **mq**-realizability, see TROELSTRA [1973a], 3.7.2(ii)). Then for a suitable t (since $\forall x^\sigma (A \vee \neg A) \leftrightarrow \forall x^\sigma \exists z ((z = 0 \wedge A) \vee (z \neq 0 \wedge \neg A))$)

$$\vdash txy = 0 \leftrightarrow Axy$$

and hence $\vdash \neg \neg \exists x^\sigma (txy = 0)$. By remark (ii) in 11.2.2,

$$\vdash (\neg \neg \exists x^\sigma (txy = 0))^D$$

implies $\vdash \exists x^\sigma (txy = 0)$, hence $\vdash \exists x^\sigma A$.

(ii) Assume for notational simplicity that $A = \forall x \exists y C(x, y)$, C quantifier-free, and let

$$\mathbf{HA}^c \vdash A \rightarrow \forall u \exists v B(u, v).$$

With the negative translation

$$\mathbf{HA} \vdash \forall x \neg \neg \exists y C(x, y) \rightarrow \forall u \neg \neg \exists v B(u, v),$$

hence

$$\mathbf{HA} \vdash \forall x \exists y C(x, y) \rightarrow \forall u \neg \neg \exists v B(u, v),$$

and so

$$\mathbf{EL} + \mathbf{AC}_{01} \vdash C(x, ax) \rightarrow \forall u \neg \neg \exists v B(u, v)$$

and therefore by the Dialectica interpretation

$$\mathbf{WE} - \mathbf{HA}^\omega \vdash C(x, ax) \rightarrow \forall u \exists v B(u, v).$$

Using ECF as a model for $\mathbf{WE} - \mathbf{HA}^\omega$:

$$\mathbf{EL} \vdash C(x, ax) \rightarrow \forall u \exists v B(u, v),$$

hence

$$\mathbf{EL} + \mathbf{AC}_{01} \vdash \forall x \exists y C(x, y) \rightarrow \forall u \exists v B(u, v).$$

By the result of GOODMAN [1968] or MINC [1975] (see 3.4) it follows that $\mathbf{HA} \vdash \forall x \exists y C(x, y) \rightarrow \forall u \exists v B(u, v)$.

(iii) Very similar: now use the Dialectica interpretation in $\mathbf{WE} - \mathbf{HA}^\omega + \mathbf{BR}_0 + \mathbf{BR}_1$ and take as a model $\mathbf{ECF}(\mathcal{U})$, $\mathcal{U}$ satisfying $\mathbf{EL} + \mathbf{BI}_0$; then use 11.8, 10.5.

(iv) From (iii) with the lemma in 6.22. $\square$

11.10. Further extensions, references

The most important extension of the Dialectica interpretation as given here is the extension to second-order arithmetic and finite type theory with set variables in GIRARD [1971, 1973]; a brief account is in TROELSTRA [1973a], 1.9.27, 3.5.21.

For a variant not requiring decidability of prime formulae in the proof of the Soundness Theorem see DILLER and NAHM [1974].

12. Local and global constructivizations of classical theorems

12.1. "Local" and "global"

From a logicians viewpoint it is certainly natural to ask whether there are general procedures which transform classical results with classical proofs into constructive results with constructive proofs. For example, such a transformation procedure should be applicable to all statements provable in a given classical system $\mathbf{H}$; after transformation of a theorem A with its proof in $\mathbf{H}$, the result should be a theorem A^* with a constructive proof in a constructively justified system $\mathbf{H}^*$.

Such a method of constructivization is here called¹ "global", in contrast to "local" constructivizations, i.e. ad hoc constructive versions of certain classical theorems which are obtained by exploiting the specific data of each theorem studied.

It stands to reason that local constructivizations, obtained utilizing the specific data of a given problem, may be expected to yield better results, in general, than global methods applied to the same problem.

There are two reasons to be interested in global constructivizations:

¹ "Global" is sometimes described as "trivial" (because obtainable by a standard method). Of course, it is not always trivial to recognize something as "trivial"!

- (1) by comparison with results obtained by global methods, one obtains a measure for the improvements obtained by local constructivizations;
- (2) even where the global constructivizations are not optimal, they can be very useful as auxiliary results (in obtaining *local* constructivizations of other theorems).

12.2. The Dialectica interpretation provides us with an example of a global constructivization method. Most of our examples given below depend on the following. The bulk of theorems in classical analysis uses only weak forms of comprehension. Assume therefore A to be a theorem such that

$$\mathbf{EL}^c + \text{ess. } \Delta_1^1\text{-CA} \vdash A.$$

If A is of the form $C \rightarrow \forall u \exists v B$, C prenex, B quantifier-free we may appeal to 11.9(iii) and obtain

$$\mathbf{EL} + \mathbf{BI}_0 + \mathbf{AC}_{01} \vdash A,$$

and if C is purely universal, with 11.9(iv),

$$\mathbf{IDB}_1 \vdash A.$$

Many theorems are in fact of the form $C \rightarrow \forall u \exists v B$, C purely universal, B quantifier-free, and all we have to do in applying the method is to verify, for a given statement, that it has the required syntactic form and that the proof does not require more than $\text{ess. } \Delta_1^1\text{-CA}$. For theorems which are not of the required form, it is often quite easy to find a slightly weaker or a classically equivalent statement which *does* have the required form; in fact, the Dialectica translation can be used to discover a suitable reformulation, see e.g. 12.4.

Up till now, the Dialectica interpretation and the closely related no-counterexample interpretation (see Chapter D.2) are the only successful methods for global constructivization. It is easy to see why the negative translation is unsatisfactory as a method of constructivization: although it establishes that classical theorems formulated in the negative fragment may be regarded as intuitionistic theorems, the method is uninteresting inasmuch the translation does not yield statements with constructive $\exists$ or $\vee$, i.e. the operations which are interesting from the viewpoint of (naive) constructivism are lacking (but cf. GEL'FOND [1972]).

Neither is realizability or modified realizability of any use, since these interpretations do not realize all instances of $A \vee \neg A$; and first applying the negative translation, then realizability does not help either, since realizability leaves negative formulae essentially unchanged. In contrast,

the Dialectica interpretation applied to negative statements introduces (constructive) $\exists$.

For another possibility of global constructivization, largely unexplored as yet, see TROELSTRA [1977a], 6.12.

12.3. Bolzano–Weierstrasz or the bisection argument

We shall assume (classical) analysis of reals and real-valued functions to be formalized in finite-type theory — so sets of natural numbers are represented by their characteristic functions of type 1, sets of reals by type 2 functionals etc.

The Bolzano–Weierstrasz theorem, and similarly the assertion that a bounded sequence of reals has a least upper bound is usually proved by means of a bisection argument which, on inspection, turns out to be formalizable with the help of arithmetic comprehension. For the existence of the l.u.b. we only have to prove the theorem for sequences of rationals, as one easily sees — therefore we restrict attention to this case. Let $\langle r_{\alpha n} \rangle_n$ enumerate a sequence of rationals contained in $[0, 1)$. Then

$$\forall k \exists! m < 2^k [\exists n (r_{\alpha n} \in [m \cdot 2^{-k}, (m+1) \cdot 2^{-k}]) \wedge \wedge \neg \exists n (r_{\alpha n} \geq (m+1) \cdot 2^{-k})].$$

Arithmetic comprehension yields a β such that

$$\forall k (\exists n (r_{\alpha n} \in [\beta k \cdot 2^{-k}, (\beta k + 1) \cdot 2^{-k}]) \wedge \neg \exists n (r_{\alpha n} \geq (\beta k + 1) \cdot 2^{-k})),$$

and $\langle \beta k \cdot 2^{-k} \rangle_k$ is an r.n.g. representing the required l.u.b.

Similarly for the Bolzano–Weierstrasz theorem.

Remark. In an unpublished manuscript, TAKEUTI [1972] shows that classical analysis can in fact be developed in a conservative extension of Peano arithmetic, obtained by introducing sets of all finite types, with arithmetical comprehension without parameters.

12.4. The intermediate-value theorem and Brouwer's fixed point theorem

We consider the following special case of the intermediate-value theorem:

$$(*) \quad \left\{ \begin{array}{l} \text{Every uniformly continuous real-valued function } f \text{ on } [0, 1] \\ \text{with } f(0) = -1, f(1) = +1 \text{ has an argument } x \in [0, 1] \text{ such} \\ \text{that } f(x) = 0. \end{array} \right.$$

A well-known classical proof proceeds as follows. Consider the set $X = \{r_n: \forall r \leq r_n (f(r) < 0)\}$ (r a variable ranging over rationals). X is a bounded non-empty subset of the rationals in $[0, 1]$, therefore has a l.u.b. $x < 1$; because of continuity arguments, $f(x) \leq 0$; but $f(x) < 0$ is excluded (again because of the continuity of f) hence $f(x) = 0$.

Now consider the following weakening of (*):

$$(**) \quad \left\{ \begin{array}{l} \text{Every uniformly continuous real-valued } f \text{ on } [0, 1] \text{ with} \\ f(0) = -1, f(1) = +1 \text{ has, for every } k, \text{ an argument } x \in [0, 1] \\ \text{such that } |f(x)| < 2^{-k}. \end{array} \right.$$

(An application of Bolzano–Weierstrasz to (**)) would yield (*).)

This can be formulated in finite-type language as follows. Let Φ be such that for any α $\langle r_{(\Phi\alpha)_n} \rangle_n$ is the corresponding r.n.g. in the standard representation of $[0, 1]$ (cf. 5.13); note that

$$|x_\alpha - r_{(\Phi\alpha)_n}| \leq 2^{-n+1}.$$

Let f be a uniformly continuous, real-valued function; f can be coded by α, β such that (writing α_x for $(\alpha)_x$) $\langle r_{(\Phi\alpha_x)_n} \rangle_n$ represents $f(r_x)$, β acts as a modulus of uniform continuity:

$$\begin{aligned} \forall nmk (0 \leq r_n \leq 1 \wedge 0 \leq r_m \leq 1 \wedge |r_n - r_m| < 2^{-\beta k} \rightarrow \\ \rightarrow |r_{(\Phi\alpha_n)(k+2)} - r_{(\Phi\alpha_m)(k+2)}| < 2^{-k}). \end{aligned} \quad (1)$$

The conditions $f(0) = -1, f(1) = +1$ are expressed by (assuming $0 = r_0, 1 = r_1$ for simplicity)

$$\forall k (|r_{(\Phi\alpha_0)k} + 1| < 2^{-k+1}), \quad \forall k (|r_{(\Phi\alpha_1)k} - 1| < 2^{-k+1}). \quad (2)$$

The conclusion of our statement can be formulated as

$$\forall k \exists n (|r_{(\Phi\alpha_n)k}| < 2^{-k}). \quad (3)$$

Therefore

$$(1) \wedge (2) \rightarrow (3)$$

can be rewritten in the form $\forall x A \rightarrow \forall u \exists v B(u, v)$, A and B quantifier-free, and this statement has been established in $\mathbf{EL}^c + \text{ess. } \Delta_1^1\text{-CA}$, and thus by 11.9(iv),

$$\mathbf{IDB}_1 \vdash (1) \wedge (2) \rightarrow (3).$$

Now this result is fairly trivial and can also be easily obtained directly (in fact, $\mathbf{EL} + \mathbf{AC}_{01}$ suffices), and is practically equivalent to (a weakened form

of) Brouwer's fixed point theorem in one dimension (cf. Remark 5.14). It is more interesting to note that exactly the same treatment applies to the following weakening of Brouwer's fixed point theorem in more dimensions:

$$\left\{ \begin{array}{l} \text{If } f \text{ is a uniformly continuous mapping from } I^n \text{ into } I^n \\ (I \equiv [0, 1]), \text{ then } \forall k \exists x \in I^n (\rho(x, fx) < 2^{-k}), \text{ where } \rho \text{ is a} \\ \text{Euclidean metric.} \end{array} \right.$$

For a classical proof of Brouwer's fixed point theorem, see e.g. ENGELKING [1968], pp. 296–304.

Let us now reconsider the constructive version of the intermediate-value theorem and show (a) how the constructive formulation can be found via the Dialectica translation and (b) how we can obtain some improvement using the Dialectica interpretation directly, not via the conservative extension result of 11.9.

The intermediate-value theorem in its classical form (*) can be expressed in the language of finite types as

$$\forall y^0 Cy \rightarrow \neg \forall \gamma \neg \forall x^0 A(\gamma, x) \quad (4)$$

where $\forall y^0 Cy$ expresses (1) $\wedge$ (2) (C quantifier-free), and $A(\gamma, x) \equiv |r_{(\Phi\alpha_{(\Phi\gamma)(\beta n)})n}| < 2^{-n+2}$. The Dialectica translation of (4) takes the form

$$\exists y^0 Y \forall X (Cy \rightarrow A(YX, X(YX)))$$

which implies

$$\forall y^0 Cy \rightarrow \exists Y \forall X A(YX, X(YX)). \quad (5)$$

Specializing X to $\lambda y^0. x^0$:

$$\forall y^0 Cy \rightarrow \exists Y \forall x^0 A(Y(\lambda y. x), x),$$

and weakening

$$\forall y^0 Cy \rightarrow \forall x^0 \exists \gamma A(\gamma, x)$$

which is equivalent to (3).

On the other hand, weakening (5) to

$$\forall y^0 Cy \rightarrow \forall X \exists \gamma A(\gamma, X\gamma)$$

and interpreting X as an (extensional) continuous functional of type 2 (acting on number-theoretic functions corresponding to r.n.g.'s), we obtain in $\mathbf{EL} + \mathbf{BI}_0 + \mathbf{AC}_{01}$:

$$\left\{ \begin{array}{l} \text{For a uniformly continuous } f \text{ on } [0, 1], f_0 = -1, f_1 = 1, \text{ and} \\ \text{for } \gamma \text{ coding an r.n.g., } X \text{ a continuous type 2 functional,} \\ \forall y^0 Cy \rightarrow \forall X^2 \exists \gamma (|fx_\gamma| < (X\gamma)^{-1}) \end{array} \right.$$

(KREISEL [1973]). A similar improvement is obtainable for Brouwer's fixed point theorem.

12.5. Weierstrasz' approximation theorem

This can be stated as follows.

$$\left. \begin{array}{l} \text{Every uniformly continuous function on } [0, 1] \text{ can be} \\ \text{approximated within } 2^{-k} \text{ by a polynomial with rational} \\ \text{coefficients, for all } k. \end{array} \right\} \quad (1)$$

Let us assume polynomials with rational coefficients to be coded onto the natural numbers; let us write P_k for the polynomial with code k . Let φ_k be the modulus of uniform continuity (on $[0, 1]$) for P_k ; we write $\varphi(k, n)$ for $\varphi_k n$. Then

$$\forall x \in I \forall y \in I (|x - y| < 2^{-\varphi(k, n)} \rightarrow |P_k x - P_k y| < 2^{-n}).$$

Assume f to be a uniformly continuous function coded by α, β ; we put $\psi_{k,n}$ for the $(\alpha)_x$ with $r_x = k \cdot 2^{-n}$ ($0 \leq k \leq 2^n$) and write

$$g(k, n, m) \equiv r_{(\Phi(\psi_{k,n}), m)}, \quad \varphi(\beta, k, n) \equiv \max\{\beta n, \varphi(k, n)\}.$$

Note that $|f(k \cdot 2^{-n}) - g(k, n, m)| < 2^{-m+1}$. It is now easy to verify that

$$\forall k \leq 2^{-\varphi(\beta, l, n+2)} (|g(k, \varphi(\beta, l, n+2), n+3) - P_l(k \cdot 2^{-\varphi(\beta, l, n+2)})| < 2^{-(n+2)}) \quad (2)$$

implies

$$\forall x \in I (|fx - P_l x| < 2^{-n}) \quad (3)$$

and that conversely (3) for $n+3$ implies (2). Therefore, if we let $\forall y^0 Cy$ stand for (1) of 12.3, we can formulate the approximation theorem as

$$\forall y^0 Cy \rightarrow \forall n \exists l (2),$$

which is of the required form.

The reader may compare this way of obtaining the Weierstrasz approximation theorem with the direct route in BISHOP [1967], p. 100.

12.6. Rolle's theorem

Another rather simple example is provided by the following weakening of Rolle's theorem:

$$(*) \quad \left\{ \begin{array}{l} \text{If } f \text{ is defined on } [0, 1] \text{ and has a uniformly continuous} \\ \text{derivative } f' \text{ on } [0, 1], \text{ and } f0 = f1 = 0, \text{ then for every } k \\ \text{there is an } x \in [0, 1] \text{ such that } |f'x| < 2^{-k}. \end{array} \right.$$

Note that (classically as well as constructively) a function with uniformly continuous derivative is itself uniformly continuous. Thus f, f' are coded by pairs α, β and α', β' respectively; $f0 = 0, f1 = 0$ is also expressed by a purely universal condition; a function γ regulates the convergence of quotients of differences to the derivative, i.e. we define " f' is a derivative of f " by the existence of a γ such that

$$x \# y \wedge |x - y| < 2^{-\gamma k} \rightarrow \left| \frac{fx - fy}{x - y} - f'x \right| < 2^{-k}.$$

We can make sure that $(\alpha, \beta), (\alpha', \beta')$ are in the relation of function and derivative by requiring

$$\forall n m k l (0 \leq r_n \leq 1 \wedge 0 \leq r_m \leq 1 \wedge r_n \neq r_m \wedge |r_n - r_m| < 2^{-\gamma k} \wedge |r_n - r_m| > 2^{-l} \rightarrow \\ \rightarrow \left| \frac{r_{(\Phi\alpha_n)(k+l)} - r_{(\Phi\alpha_n)(k+l)}}{r_n - r_m} - r_{(\Phi\alpha'_n)k} \right| < 2^{-k+3}).$$

Now we can again apply our conservative extension result, which yields the existence of a constructive proof of Rolle's theorem as stated in (*).

12.7. Still further examples can be found e.g. in KREISEL [1952], where certain classical theorems concerning power series (in real or complex variables) are reformulated.

12.8. Example of a "local" constructivization

Although the weakened version of the intermediate-value theorem described above is sometimes useful, it is mathematically more interesting to find additional conditions to be added to the premiss of the intermediate-value theorem which permit us to maintain the original strong conclusion. One such rather obvious additional condition is the following (BISHOP [1967], p. 59, Exercise 14)

$$\forall kl (0 \leq r_k \leq 1 \wedge 0 \leq r_l \leq 1 \wedge r_k < r_l \rightarrow \exists ij (r_k < r_i < r_l \wedge |f r_i| > 2^{-j})) \quad (1)$$

or, what amounts to the same,

$$\forall xy [x < y \wedge x \in [0, 1] \wedge y \in [0, 1] \rightarrow \exists z \in [x, y] (|fz| > 0)].$$

The additional condition (1) enables us to apply a standard bi-section argument:

Put $[x_0, y_0] = [0, 1]$. Let $r_i \in [\frac{1}{4}, \frac{3}{4}]$ be such that $f r_i \neq 0$; if $f r_i < 0$, take $[x_1, y_1] = [r_i, 1]$, $[0, r_i]$ otherwise. Assume $[x_n, y_n]$ to be constructed; let $r_j \in [\frac{3}{4}x_n + \frac{1}{4}y_n, \frac{1}{4}x_n + \frac{3}{4}y_n]$ be such that $f r_j \neq 0$; if $f r_j < 0$, put $[x_{n+1}, y_{n+1}] = [r_j, y_n]$, $[x_n, r_j]$ otherwise. It is easy to see that $\langle [x_n, y_n] \rangle_n$ converges to a single point; $f x_n < 0$, $f y_n > 0$ for all n , hence for the limit x , $f x = 0$.

Of course, it remains to be shown that (1) is a property possessed by most of the "usual" functions. For example, one can show the following.

If f is $n+1$ times uniformly differentiable, with derivatives $f^{(1)}, f^{(2)}, \dots, f^{(n+1)}$, and $C > 0$ is a constant such that on $[a, b]$ ($a < b$)

$$|f x| + |f^{(1)} x| + \dots + |f^{(n)}(x)| > C$$

is satisfied, then (1) holds. (1) is also true for strictly increasing or decreasing functions.

References*

BEESON, M.J.

- [1975] The nonderivability in intuitionistic formal systems of theorems on the continuity of effective operations, *J. Symbolic Logic*, **40**, 321–346.

BENACERRAF, P. and H. PUTNAM, editors

- [1964] *Philosophy of Mathematics, Selected Readings* (Prentice-Hall, Englewood Cliffs, NJ).

BETH, E.W.

- [1959] *The Foundations of Mathematics* (North-Holland, Amsterdam, 2nd. revised ed. 1965, reprinted 1968).

BISHOP, E.

- [1967] *Foundations of Constructive Analysis* (McGraw Hill, New York).

BROUWER, L.E.J.

- [1924] Intuitionistische Zerlegung mathematischer Grundbegriffe, *Jber. Deutsch. Math. Verein*, **33**, 251–256.
 [1949] Consciousness, philosophy and mathematics, in: *Proceedings of the 10th International Congress on Philosophy*, Amsterdam 1948, edited by E.W. Beth and H.J. Pors (North-Holland, Amsterdam) pp. 1235–1249.

*The following sources contain extensive bibliographies: HEYTING [1955, 1956], KLEENE [1952], KLEENE and VESLEY [1965], TROELSTRA [1973, 1977a] (all on intuitionism), ŠANIN [1962], KUŠNER [1973] (on CRA). See also the section on constructive mathematics in the *Zentralblatt für Mathematik*.

- [1952] Historical background, principles and methods of intuitionism, *South African J. Sci.*, **49**, 139–146.
- [1954] Points and spaces, *Canad. J. Math.*, **6**, 1–17.
- [1975] *Collected Works*, Vol. I, edited by A. Heyting (North-Holland, Amsterdam).
- CEITIN, G.S.
 - [1959] Algorithmic operators in constructive complete separable metric spaces (Russian), *Doklady Akad. Nauk*, **128**, 49–52.
- DALEN, D. VAN
 - [1973] Lectures on intuitionism, in: *Cambridge Summer School in Mathematical Logic*, edited by A.R.D. Mathias and H. Rogers (Springer, Berlin) pp. 1–94.
- DILLER, J. and W. NAHM
 - [1974] Eine Variante zur Dialectica Interpretation der Heyting-Arithmetik endlicher Typen, *Arch. Math. Logik. Grundlagenforschung*, **16**, 49–66.
- DRAGALIN, A.G.
 - [1973] Constructive mathematics and models of intuitionistic theories, in: *Logic, Methodology and Science IV*, edited by P. Suppes et al. (North-Holland, Amsterdam) pp. 111–128.
- DYSON, V.H. and G. KREISEL
 - [1961] Analysis of Beth's semantic construction of intuitionistic logic, Technical Report 3, Applied Mathematics and Statistics Laboratories, Stanford University, Stanford, CA.
- ENGELKING, R.
 - [1968] *Outline of General Topology* (North-Holland, Amsterdam/PWN — Polish Scientific Publishers, Warsaw/Wiley, New York).
- FITTING, M.
 - [1969] *Intuitionistic Logic, Model Theory and Forcing* (North-Holland, Amsterdam).
- FRIEDMAN, H.
 - [1973] Some applications of Kleene's methods for intuitionistic systems, in: *Cambridge Summer School in Mathematical Logic*, edited by A.R.D. Mathias and H. Rogers (Springer, Berlin).
- GEL'FOND, M.G.
 - [1972] O sootnošenii klassičeskogo i konstruktivnogo variantov postroeniya matematičeskogo analiza (On the relation between classical and constructive analysis), *Zap. Naučn. Sem. Otdel. Math. Inst. Steklov (LOMI)*, **32**, 5–11 (Russian).
- GENTZEN, G.
 - [1969] On the relation between intuitionist and classical arithmetic, in: *The Collected Papers of Gerhard Gentzen*, edited by M.E. Szabo (North-Holland, Amsterdam) pp. 53–67.
- GIRARD, J.Y.
 - [1971] Une extension de l'interprétation de Gödel à l'analyse, et son application à l'élimination des coupures dans l'analyse et la théorie des types, in: *Proceedings of the Second Scandinavian Logic Symposium*, edited by J.E. Fenstad (North-Holland, Amsterdam) pp. 63–92.
 - [1973] Quelques résultats sur les interprétations fonctionnelles, in: *Cambridge Summer School in Mathematical Logic*, edited by A.R.D. Mathias and H. Rogers (Springer, Berlin) pp. 232–252.
- GÖDEL, K.
 - [1933] Zur intuitionistischen Arithmetik und Zahlentheorie, in: *Ergebnisse eines mathematische Kolloquiums*, **4**, 34–38. [English translation: On intuitionistic arithmetic and number theory, in: *The Undecidable*, edited by M. Davis (Raven Press, New York) pp. 75–81.]

- [1958] Ueber eine bisher noch nicht benützte Erweiterung des finiten Standpunktes, *Dialectica*, **12**, 280–287.
- GOODMAN, N.D.
 [1968] Intuitionistic arithmetic as a theory of constructions, Ph.D. Thesis, Stanford University, Stanford, CA.
- HEYTING, A.
 [1931] Die intuitionistische Grundlegung der Mathematik, *Erkenntnis*, **2**, 106–115.
 [1954] Logique et intuitionnisme, in: *Actes du 2^e Colloque Internationale de Logique Mathématique, Paris 1952* (Paris).
 [1955] *Les fondements des mathématiques. Intuitionnisme. Théorie de la démonstration* (Gauthier-Villars, Paris/Nauwelaerts, Louvain).
 [1956] *Intuitionism, an Introduction* (North-Holland, Amsterdam, 2nd revised ed. 1966; 3rd revised ed. 1972).
- HILBERT, D. and P. BERNAYS
 [1934] *Grundlagen der Mathematik I* (Springer, Berlin, 2nd revised ed. 1968).
- HINATA, S.
 [1967] Calculability of primitive recursive functionals of finite type, *Science reports of the Tokyo Kyoiku Daigaku A*, **9**, 218–235.
- HOWARD, W.A.
 [1968] Functional interpretation of bar induction by bar recursion, *Compositio Math.*, **20**, 107–124.
 [1970] Assignment of ordinals to terms for primitive recursive functionals of finite type, in: *Intuitionism and Proof Theory*, edited by A. Kino, J. Myhill and R.E. Vesley (North-Holland, Amsterdam) pp. 443–458.
 [1973] Hereditarily majorizable functions of finite type, in: TROELSTRA [1973a] pp. 454–461.
- HOWARD, W.A. and G. KREISEL
 [1966] Transfinite induction and bar induction of types zero and one, and the role of continuity in intuitionistic analysis, *J. Symbolic Logic*, **31**, 325–358.
- JONGH, D.H.J. DE
 [1973] Formulas in one propositional variable in intuitionistic arithmetic, Report 73–03, Dept. of Math., University of Amsterdam.
- KLEENE, S.C.
 [1945] On the interpretation of intuitionistic number theory, *J. Symbolic Logic*, **10**, 109–124.
 [1952] *Introduction to Metamathematics* (North-Holland, Amsterdam/P. Noordhoff, Groningen/D. van Nostrand, New York).
 [1959] Countable functionals, in: *Constructivity in Mathematics*, edited by A. Heyting (North-Holland, Amsterdam) pp. 81–100.
 [1960] Realizability and Šanin's algorithm for the constructive deciphering of mathematical sentences, *Logique et Analyse*, **3**, 154–165.
 [1962] Disjunction and existence under implication in elementary intuitionistic formalisms, *J. Symbolic Logic*, **27**, 11–18.
 [1963] An addendum, *J. Symbolic Logic*, **28**, 154–156.
 [1969] Formalized recursive functionals and formalized realizability, *Mem. Am. Math. Soc.*, **89**.
- KLEENE, S.C. and R.E. VESLEY
 [1965] *The Foundations of Intuitionistic Mathematics, Especially in Relation to Recursive Functions* (North-Holland, Amsterdam).
- KOLMOGOROV, A.N.
 [1925] O principe tertium non datur (On the principle of tertium non datur), *Mat. Sb.*, **32**, 646–667 (Russian). [English translation in: *From Frege to Gödel*, edited by J. van Heijenoort (Harvard University Press, Cambridge, MA, 1967) pp. 416–437.]

KREISEL, G.

- [1952] Some elementary inequalities, *Indag. Math.*, **14**, 334–338.
- [1958] Mathematical significance of consistency proofs, *J. Symbolic Logic*, **23**, 155–182.
- [1959] Interpretation of analysis by means of constructive functionals of finite type, in: *Constructivity in Mathematics*, edited by A. Heyting (North-Holland, Amsterdam) pp. 101–128.
- [1962] On weak completeness of intuitionistic predicate logic, *J. Symbolic Logic*, **27**, 139–158.
- [1965] Mathematical logic, in: *Lectures on Modern Mathematics*, III, edited by T. L. Saaty (Wiley, New York) pp. 95–195.
- [1968] Functions, ordinals, species, in: *Logic, Methodology and Philosophy of Science III*, edited by J.F. Staal and B. van Rootselaar (North-Holland, Amsterdam) pp. 145–159.
- [1970] Church's thesis: A kind of reducibility axiom for constructive mathematics, in: *Intuitionism and Proof Theory*, edited by A. Kino, J. Myhill and R.E. Vesley (North-Holland, Amsterdam) pp. 121–150.
- [1972] Which number theoretic problems can be solved in recursive progressions on Π -paths through 0? *J. Symbolic Logic*, **37**, 311–334.
- [1973] The need for abstract methods in mathematics: a topic for proof theory, unpublished lecture.

KREISEL, G. and J.L. KRIVINE

- [1966] *Éléments de logique mathématique* (Dunod, Paris). [Revised English ed.: *Elements of Mathematical Logic* (North-Holland, Amsterdam 1967); Revised German ed.: *Modelltheorie* (Springer, Berlin, 1972).]

KREISEL, G. and A.S. TROELSTRA

- [1970] Formal systems for some branches of intuitionistic analysis, *Ann. Math. Logic*, **1**, 229–387.

KRIPKE, S.

- [1965] Semantical analysis of intuitionistic logic I, in: *Formal Systems and Recursive Functions*, edited by J.N. Crossley and M.A.E. Dummett (North-Holland, Amsterdam) pp. 92–130.

KUŠNER, B.A.

- [1973] *Lekcii po Konstruktivnomu Matematičeskomu Analizu* (Lectures on constructive mathematical analysis) (Russian) (Nauka, Moscow).

MARKOV, A.A.

- [1962] On constructive mathematics, *Trudy Mat. Inst. Steklov*, **67**, 8–14. (Russian) [English translation in *Am. Math. Soc. Transl.*, **98** (2) (1971) 1–9.]
- [1971] Essai de construction d'une logique de la mathématique constructive, *Rev. Internat. Philos*, **98**, 477–507.
- [1974] On the language ya_0 , *Dokl. Akad. Nauk SSSR*, **214**, 40–43 (Russian). [= *Sov. Math. Dokl.*, **15**, 38–40.]
- On the language ya_1 , *Dokl. Akad. Nauk SSSR*, **214**, 279–282. [= *Sov. Math. Dokl.*, **15**, 125–129.]
- On the language ya_2 , *Dokl. Akad. Nauk SSSR*, **214**, 513–516. [= *Sov. Math. Dokl.*, **15**, 184–189.]
- On the language ya_3 , *Dokl. Akad. Nauk SSSR*, **214**, 765–768. [= *Sov. Math.* **15**, 242–247.]
- On the language $ya_4, ya_5, \dots$, *Dokl. Akad. Nauk SSSR*, **214**, 1030–1034. [= *Sov. Math. Dokl.*, **15**, 313–318.]
- On the language ya_ω , *Dokl. Akad. Nauk SSSR*, **214**, 1265–1268. [= *Sov. Math. Dokl.*, **15**, 356–360.]

- On the language $\mathcal{Y}_{\omega_1}$, *Dokl. Akad. Nauk SSSR*, **215**, 57–60. [= *Sov. Math. Dokl.*, **15**, 443–448.]
- MARTIN-LÖF, P.
 [1970] *Notes on Constructive Mathematics* (Almqvist and Wiksell, Stockholm).
 [1975] An intuitionistic theory of types: predicative part, in: *Logic Colloquium '73*, edited by H.E. Rose and J.C. Shepherdson (North-Holland, Amsterdam) pp. 73–118.
- MAYOH, B.
 [1965] Unsolvable problems in the theory of computable numbers, in: *Formal Systems and Recursive Functions*, edited by J.N. Crossley and M.A.E. Dummett (North-Holland, Amsterdam) pp. 272–279.
- MINC, G.E.
 [1975] Finitnoe issledovanie transfinitnyh vyvodov (Finite investigation of infinite derivations) *Zap. Naučn. Sem. Leningrad. Otdel. Math. Inst. Steklov (LOMI)*, **49**, 67–122 (Russian, with English summary).
- MINC, G.E. and V.P. OREVKOV
 [1967] On imbedding operators, *Zap. Naučn. Sem. Leningrad. Otdel. Math. Inst. Steklov (LOMI)*, **4**, 160–167 (Russian). [English translation in *Sem. Math. V.A. Steklov Math. Inst. Leningrad*, **4** (1969) 64–66.]
- MOSCHOVAKIS, J.R.
 [1973] A topological interpretation of second-order intuitionistic arithmetic, *Compositio Math.*, **26**, 261–275.
- MOSCHOVAKIS, Y.N.
 [1964] Recursive metric spaces, *Fund. Math.*, **55**, 215–238.
 [1965] Notation systems and recursive ordered fields, *Compositio Math.*, **17**, 40–71.
- NAGASHIMA, T.
 [1966] An extension of the Craig–Schütte interpolation theorem, *Ann. Japan Assoc. Philos. Sci.*, **3**, 12–18.
- OREVKOV, V.P.
 [1963] A constructive map of the square into itself, which moves every constructive point, *Dokl. Akad. Nauk. SSSR*, **152**, 55–58 (Russian). [English translation in *Soviet Mathematics*, **4** (1963) 1253–1256.]
 [1964] On constructive mappings of a circle into itself, *Trudy Mat. Inst. Steklov*, **72**, 437–461 (Russian). [English translation in *Am. Math. Soc. Trans.*, **100**, 69–100.]
- PRAWITZ, D.
 [1965] *Natural Deduction, a Proof-Theoretical Study* (Almqvist and Wiksell, Stockholm).
- RASIOWA, H. and R. SIKORSKI
 [1963] *The Mathematics of Metamathematics* (PWN — Polish Scientific Publishers, Warsaw).
- ŠANIN, N.A.
 [1958] On the constructive interpretation of mathematical judgments, *Trudy Mat. Inst. Steklov*, **52**, 226–311 (Russian). [English translation in *Am. Math. Soc. Transl.*, **23** (2) (1963) 109–189.]
 [1962] Constructive real numbers and constructive function spaces, *Trudy Mat. Inst. Steklov*, **67**, 15–294 (Russian). [English translation in *Translations of Mathematical Monographs*, Vol. 21 (A.M.S. Providence, RI, 1968).]
 [1964] Concerning the constructive interpretation of auxiliary formulas I, *Trudy Mat. Inst. Steklov*, **72**, 348–379 (Russian). [English translation in *Am. Math. Soc. Transl.*, **99** (2) (1972) 233–275.]
 [1974] Ob ierarhii sposobov ponimanya suzhenii v konstruktivnoi matematike (On the hierarchy of ways of understanding sentences in constructive mathematics), *Trudy Mat. Inst. Steklov*, **129**, 203–206 (Russian).

SCHÜTTE, K.

- [1962] Der Interpolationssatz der intuitionistischen Prädikatenlogik, *Math. Ann.*, **148**, 192–200.

SCOTT, D.S.

- [1968] Extending the topological interpretation to intuitionistic analysis, *Compositio Math.* **20**, 194–210.
 [1970] Extending the topological interpretation to intuitionistic analysis II, in: *Intuitionism and Proof Theory*, edited by A. Kino, J. Myhill and R.E. Vesley (North-Holland, Amsterdam) pp. 235–255.

SMORYNSKI, C.A.

- [1973a] Applications of Kripke models, in: TROELSTRA [1973a] Ch. V, pp. 324–391.
 [1973b] Elementary intuitionistic theories, *J. Symbolic Logic*, **38**, 102–134.

SPECTOR, C.

- [1962] Provably recursive functionals of analysis: a consistency proof of analysis by an extension of principles formulated in current intuitionistic mathematics, in: *Proceedings of the Symposia in Pure Mathematics V*, edited by J.C.E. Dekker (A.M.S., Providence, RI) pp. 1–27.

TAIT, W.W.

- [1967] Intensional interpretations of functionals of finite type I, *J. Symbolic Logic*, **32**, 198–212.

TAKEUTI, G.

- [1972] A conservative extension of Peano arithmetic, mimeographed. University of Heidelberg.

TROELSTRA, A.S.

- [1969] *Principles of Intuitionism* (Springer, Berlin).
 [1971] Notions of realizability for intuitionistic arithmetic and intuitionistic arithmetic in all finite types, in: *Proceedings of the Second Scandinavian Logic Symposium*, edited by J.E. Fenstad (North-Holland, Amsterdam) pp. 369–405. [Errata in *Zentralblatt*, **227** (02015); bibliography of TROELSTRA [1973a].]
 [1973a] (editor), *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*, Lecture Notes in Mathematics, Vol. 344 (Springer, Berlin).
 [1973b] Notes on intuitionistic second order arithmetic, in: *Cambridge Summer School in Mathematical Logic*, edited by A.R.D. Mathias and H. Rogers (Springer, Berlin) pp. 171–205.
 [1974] Note on the fan theorem, *J. Symbolic Logic*, **39**, 584–596.
 [1975] Non-extensional equality, *Fund. Math.*, **82**, 307–322.
 [1977a] *Choice Sequences, a Chapter of Intuitionistic Mathematics* (Clarendon Press, Oxford).
 [1977b] Completeness and validity for intuitionistic predicate logic, in: *Proceedings of the "Séminaire international d'été et Colloque international de Logique à Clermont-Ferrand*, July 1975.

WEYL, H.

- [1918] *Das Kontinuum. Kritische Untersuchungen über die Grundlagen der Analysis* (Gruyter, Leipzig, reprinted 1932).

The Logic of Topoi

MICHAEL P. FOURMAN

Contents

1. Introduction	1054
2. Category-theoretic preliminaries	1055
3. The logic of partial elements	1058
4. Categories from logic	1065
5. Topoi	1068
6. Logical constructs in topos	1071
7. Interpretations in topos	1076
8. Topoi as theories	1083
References	1089

1. Introduction

The purpose of this chapter is to give an expository presentation of the correspondence between topoi and theories which makes precise Lawvere's claim that "the notion of topos summarises in objective categorical form the essence of 'higher-order logic'" (LAWVERE [1975]). Elementary topoi turn out to correspond to *theories* in a quite natural logic, formally an *intuitionistic type theory* (with the full comprehension axiom). The theories in question are definitionally complete theories (this notion is defined in Section 6) and *every* theory has an obvious definitional completion. To assert that topoi correspond to theories is not to deny that certain topoi may be viewed as models for our logic. Models may be described syntactically by "diagrams" so theories may be said to *include* models. Our point is that, in general, topoi may be viewed as theories. In particular, some topoi which *arise* semantically are better understood as theories than as models. Thus we regard topos theory as the "algebraic" form of this higher-order intuitionistic logic.

The formalization of our logic was developed in joint seminars with Dana Scott in 1973. The connection with topoi was first described by the author at an informal session of the 1974 Séminaire de Mathématiques Supérieures in Montréal and formed the basis of his thesis (FOURMAN [1974]). Formal systems corresponding to topoi have been described independently by other authors, notably COSTE [1974] and BOILEAU [1975]. Their systems lack the main innovation of our formalization — an *existence predicate* — and they are therefore forced to make awkward restrictions on the rule of *modus ponens*. As LAWVERE [1975] has observed, these restrictions are occasioned by a shortcoming in the traditional interpretation of variables. We *emphatically* do not agree that because of this "the traditional logical way of dealing with variables . . . should be abandoned". The traditional use of variables has much to commend it and there are far less drastic remedies to hand.

The primary purpose of introducing an existence predicate is to formalize in a natural way the logic of *partial elements* (in the case of sheaves these are the possibly non-global sections). By modifying the interpretation of *free* variables (allowing them to range over partial elements) we may continue to deal with variables in the accustomed way, retaining the fundamental *transitivity of entailment*. The various formal systems corresponding to topoi are of course formally intertranslatable (via topoi if you like). It is thus largely a matter of taste which is preferred.

A further aim of this chapter is to give a presentation of topoi accessible

to logicians. It was Lawvere's realization that certain logical constructs (e.g. the formation of power-types) could be interpreted in categories of sheaves — Grothendieck topoi — which led to the axiomatization of elementary topoi (LAWVERE [1970], LAWVERE and TIERNEY [1970]). We believe that a thorough understanding of Lawvere's insight will enable logicians to exploit the many models provided by Grothendieck and his co-workers (see e.g. ARTIN, GROTHENDIECK and VERDIER [1972]). These should be useful not only in the study of pure logic but also in finding applications of logic extending the non-set-theoretical uses of Boolean-valued models (see SCOTT [1969], TAKEUTI [1977] and ROUSSEAU [1977]).

I am grateful to Dana Scott for many stimulating conversations and for his detailed and constructive criticisms of this work in all its stages.

2. Category-theoretic preliminaries

The concepts we require from category theory are quite elementary. We review them here since even in introductory texts they are often presented with a certain degree of sophistication. If we avoid using general notions such as *limit* and *adjoint*, this is not because we consider them unimportant. For our present purposes, however, it is necessary to spell out the elementary properties (in terms of objects and morphisms) which are all too often hidden by the abstract definitions. For a more general discussion which exhibits the underlying unity of many seemingly diverse constructs see MAC LANE [1971] (especially Chapters III and IV).

We assume that the reader knows what categories and functors (homomorphisms of categories) are. We shall confuse notationally an object A with its identity morphism $A : A \rightarrow A$. Given morphisms $f : A \rightarrow B$ and $g : B \rightarrow C$ we write the composition in the order $g \circ f : A \rightarrow C$.

2.1. DEFINITION. A category with *finite products* has firstly a *terminal object* $\mathbf{1}$ (the product of the empty family) with the property that there is a unique morphism $A \rightarrow \mathbf{1}$ from each object A to it, and secondly for each pair A, B of objects, a *product* $A \times B$ equipped with projections π_1, π_2 such that for each pair of morphisms $f : C \rightarrow A$ and $g : C \rightarrow B$ there is a unique morphism $\langle f, g \rangle : C \rightarrow A \times B$ making the diagram commute.

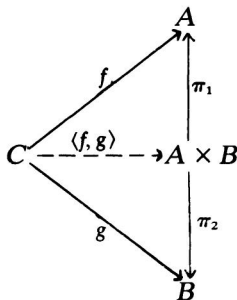


Diagram 1.

We write $h \times k$ for $\langle h \circ \pi_1, k \circ \pi_2 \rangle : A \times B \rightarrow C \times D$ where $h : A \rightarrow C$ and $k : B \rightarrow D$.

Remark. In a sense the concept of a category with finite products is *equational* (or essentially algebraic). The *commutativity* of the above diagram amounts to having the two equations:

$$\pi_1 \circ \langle f, g \rangle = f, \quad \pi_2 \circ \langle f, g \rangle = g.$$

The *uniqueness* of $\langle f, g \rangle$ amounts to having the further equation

$$\langle \pi_1 \circ h, \pi_2 \circ h \rangle = h.$$

To make this precise requires a consideration of algebras with *partial operations* (a category with finite products is just such an algebra, see SCOTT [1975]). Similar remarks apply to the following concepts: *category*, *category with finite limits*, *cartesian-closed category* and *topos*.

2.2. DEFINITION. A category is *cartesian closed* if it has finite products and for each pair A, B of objects, we have an *exponent* B^A and *evaluation morphism*

$$\text{ev} : A \times B^A \rightarrow B$$

such that for any $f : A \times X \rightarrow B$ there is a unique $\hat{f} : X \rightarrow B^A$ with

$$\text{ev} \circ A \times \hat{f} = f$$

(the uniqueness may be imposed equationally by $(\text{ev} \circ A \times g)^\wedge = g$). We call $\hat{f}$ the *transpose* of f and *vice versa*.

2.3. DEFINITION. In an arbitrary category, given morphisms $f, g : A \rightarrow B$

we say that $e : X \rightarrow A$ is an *equalizer* of f and g iff not only $f \circ e = g \circ e$, but also for any $h : Y \rightarrow A$ with $f \circ h = g \circ h$ there is a unique $k : Y \rightarrow X$ with $e \circ k = h$. In this case

$$X \xrightarrow{e} A \begin{matrix} \xrightarrow{f} \\ \xrightarrow{g} \end{matrix} B$$

is said to be an *equalizer diagram*.

2.4. DEFINITION. The square (f, f', g, g') in the diagram is said to be a

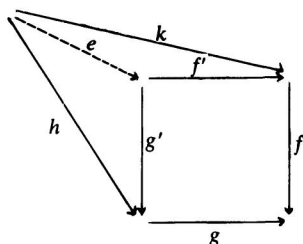


Diagram 2.

pullback iff not only $f \circ f' = g \circ g'$ but also for any pair k, h of morphisms such that $f \circ k = g \circ h$ there is a unique morphism e such that $f' \circ e = k$ and $g' \circ e = h$.

The reader should make precise and prove the assertion that terminal objects, products, exponents, equalizers and pullbacks are unique up to a unique isomorphism.

2.5. DEFINITION. A morphism f is a *monomorphism* iff whenever $f \circ g = f \circ h$, then $g = h$. Monomorphisms (briefly monos) are said to be *monic*. If f and k are monos with common codomain A we say that $f \leq k$ iff f factors through k ; that is, $f = k \circ g$ for some morphism g . If $f \leq k$ and $k \leq f$, we say that f and k represent the same *subobject* of A . We write $\mathcal{P}(A)$ for the (partially ordered) class of subobjects of A .

The proof of the basic facts in the following proposition is left to the reader.

2.6. PROPOSITION. (1) *Every equalizer is monic.*

(2) *If f is monic, then $\langle f, g \rangle$ is monic.*

(3) If

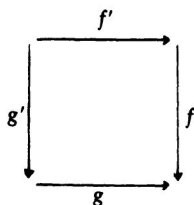


Diagram 3.

is a pullback and g is monic so is f' .

(4) If both small squares are pullbacks, so is the outer rectangle.

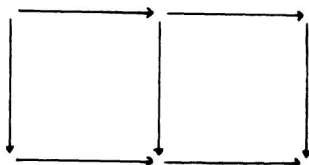


Diagram 4.

(5) If a category has finite products and equalizers (i.e. every pair of morphisms $f, g : A \rightarrow B$ has an equalizer), then it has pullbacks (i.e. from every pair of morphisms with common codomain we can construct a pullback).

2.7. DEFINITION. A category is *finitely complete* iff it has finite products and equalizers. (The point here is that such a category has limits for *all* finite diagrams, see MAC LANE [1971].)

3. The logic of partial elements

Standard formalizations of logic are valid only for non-empty domains. Classically we imagine we can decide whether a domain is empty or not. Even intuitionistically, so long as we treat only one domain we lose nothing by assuming it “inhabited”. If, however, we want to consider the subdomain determined by an undecidable predicate, we must say that it may be undecidable whether a given x *exists qua* element of the subdomain. Thus in general as soon as we deal with more than one sort we find we must adapt our logic to deal with domains of which we can neither decide

whether they are inhabited, nor whether their elements exist fully. When we talk about something, we cannot always presuppose its existence. Well-formed terms of a language may fail to denote. Many kinds of “free” logic have been suggested for classical systems but the problem of existence only becomes acute in an intuitionistic framework where we may no longer assert that a domain must be *either* inhabited *or* empty.

To deal with terms which may not denote we introduce a formal *existence predicate* **E**. We read **E** τ as “ τ exists”. One may think of free variables of sort *A* as ranging over an (implicit) outer domain of potential elements. (We shall see later how any domain *A* of partial elements may be represented as a subdomain of a domain $\tilde{A}$ of total elements which we may think of objectifying the potential elements of *A*.) The predicate **E** then picks out the subdomain *A* of actual elements. We modify Quine’s *dictum* to “to be is to be the value of a *bound* variable” by regarding bound variables as *restricted* to **E**. Bound variables range only over actual elements.

Whenever one introduces a domain, one must also introduce a notion of *sameness* within that domain. There is a notion of *equality* of partial elements which presupposes existence in the following sense:

$$\tau = \sigma \rightarrow \mathbf{E}\tau \wedge \mathbf{E}\sigma.$$

We also introduce a notion of *equivalence*, essentially by considering all elements outside **E** as equivalent in their non-existence. Intuitionistically, we must phrase this more positively and express equivalence by

$$\tau \equiv \sigma \leftrightarrow (\mathbf{E}\tau \rightarrow \tau = \sigma) \wedge (\mathbf{E}\sigma \rightarrow \tau = \sigma).$$

This relation is basic to our logic. We banish any possible intensional notions by requiring that equivalent elements be indistinguishable. Well-defined predicates should be extensional not only with respect to equality but also with respect to equivalence. This extensionality is expressed by the schema

$$\varphi[\tau/x] \wedge \tau \equiv \sigma \rightarrow \varphi[\sigma/x].$$

Since $\equiv$ is so fundamental we take $\equiv$ and **E** as primitives and define equality by

$$\tau = \sigma \leftrightarrow \tau \equiv \sigma \wedge \mathbf{E}\tau \wedge \mathbf{E}\sigma.$$

We present the logic as a *many-sorted* theory with *higher types*. To give the higher-order structure it is sufficient to have a map which assigns to each finite sequence $(A_0, \dots, A_{n-1})$ of sorts a sort $[A_0, \dots, A_{n-1}]$ which we think of as the “power sort” of all *n*-ary relations on the given sequence of

domains. As we shall see other type constructs are reducible to ideas defined in terms of these power sorts. The axiomatization of higher-order logic is simplified by the fact that it suffices to take *conjunction*, *implication* and *universal quantification* as the only primitive logical connectives: the other connectives are definable in terms of these.

It was suggested by Scott that, having introduced the existence predicate, it is convenient and straightforward to employ *definite descriptions* as terms. We do this as it gives us a conveniently large stock of terms. The term $\mathbf{!}x\varphi$ is to be read “the unique x such that φ ”. A fuller discussion of the intuitionistic logic of partial elements and descriptions may be found in SCOTT [1977] and FOURMAN and SCOTT [1977]. We now turn to a presentation of the formalization of this logic.

3.1. DEFINITION. A *higher-order language* is specified by the following data:

(1) Two sets Sort and Const (of sorts and constants).

(2) A *power-type map* from $\bigcup_{n \in \omega} \text{Sort}^n$ to Sort written as $(A_0, \dots, A_{n-1}) \mapsto [A_0, \dots, A_{n-1}]$.

(3) A map assigning a sort to each constant, $\# : \text{Const} \rightarrow \text{Sort}$.

Given a language, we introduce a set Var of *variables*. Each variable x has a sort $\#x$. There are countably many variables of each sort.

To avoid confusion we point out that we do not assume that the sorts are built up syntactically from a set of “ground-sorts” by iterating the power-type operation. In particular it is not assumed that $[A] = [B]$ implies $A = B$. This “abstractness” poses no real problems.

3.2. DEFINITION. The sets of *terms* $(\tau, \sigma, \dots)$ and *formulae* $(\varphi, \psi, \dots)$ of a language are sets of expressions built up inductively according to the scheme opposite. Each term τ is assigned a sort $\#\tau$ and the inclusion of an expression is conditional on the proviso’s being satisfied.

We leave it to the reader to define the set of *free variables* of a term or formula ($\text{FV}(\tau)$ and $\text{FV}(\varphi)$ respectively), and the result of *substituting* a term σ for a variable x (where $\#\sigma = \#x$) in a term or formula, $(\tau[\sigma/x]$ and $\varphi[\sigma/x]$ respectively). For convenience we assume that the substitution operation changes bound variables as necessary to avoid clashes. We make free use of customary abbreviations, in particular we write $\forall \bar{x}$ for a finite string of quantifiers (including the empty string), $\mathbb{A}$ for a finite conjunction and $\varphi \leftrightarrow \psi$ for $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

	Expression	Sort	Proviso
Terms:	x	$\#x$	$x \in \text{Var}$
	c	$\#c$	$c \in \text{Const}$
	$\mathbf{I}x \varphi$	$\#x$	$x \in \text{Var}, \varphi$ a formula

	Expression	Proviso
Formulae:	$\mathbf{E}\tau$	τ a term
	$\tau \equiv \sigma$	$\#\tau = \#\sigma$
	$\tau(\sigma_0, \dots, \sigma_{n-1})$	$\#\tau = [\#\sigma_0, \dots, \#\sigma_{n-1}]$
	$(\varphi \wedge \psi)$	φ, ψ formulae
	$(\varphi \rightarrow \psi)$	φ, ψ formulae
	$\mathbf{V}x \varphi$	$x \in \text{Var}, \varphi$ a formula

We note here that the empty sequence of sorts gives rise to the special power sort $[]$ which can be regarded as consisting of truth values. If τ is a term of sort $[]$, then $\tau()$ is a formula which in effect *asserts* the proposition τ .

3.3. DEFINITION. As *axioms* and *rules* we take those instance of the following schemata which are well-formed.

$$(\text{Propositional axioms}) \quad \left\{ \begin{array}{l} \varphi \rightarrow (\psi \rightarrow \varphi), \\ (\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta)), \\ (\varphi \wedge \psi) \rightarrow \varphi, \\ (\varphi \wedge \psi) \rightarrow \psi, \\ (\varphi \rightarrow (\psi \rightarrow (\varphi \wedge \psi))); \end{array} \right.$$

$$\begin{aligned} \text{Axioms:} \quad & (\equiv) \quad \varphi[y/x] \wedge y \equiv z \rightarrow \varphi[z/x], \\ & (\text{E}) \quad \mathbf{V}x (x \equiv y \leftrightarrow x \equiv z) \rightarrow y \equiv z, \\ & (\mathbf{V}) \quad \mathbf{V}x \varphi \wedge \mathbf{E}x \rightarrow \varphi, \\ & (\mathbf{I}) \quad \mathbf{V}y (y \equiv \mathbf{I}x \varphi \leftrightarrow \mathbf{V}x (\varphi \leftrightarrow x \equiv y)), \\ \text{Comp} \quad & \mathbf{E}\mathbf{I}y \mathbf{V}\bar{x} (\varphi \leftrightarrow y(\bar{x})), \\ \text{Pred} \quad & y(\bar{x}) \rightarrow \mathbf{E}y \wedge \mathbf{M} \mathbf{E}x_i. \end{aligned}$$

$$(\text{MP}) \quad \frac{\varphi \quad \varphi \rightarrow \psi}{\psi}, \quad (\text{Sub}) \quad \frac{\varphi}{\varphi[\tau/x]},$$

Rules:

$$(\mathbf{V}^+) \quad \frac{\psi \wedge \mathbf{E}x \rightarrow \varphi}{\psi \rightarrow \mathbf{V}x \varphi}, \quad \text{where } x \notin \text{FV}(\psi).$$

The *propositional axioms* are those standard for intuitionistic logic. Axiom ($\equiv$) is the principle of *substitutivity* of equivalents. The *extensionality* axiom (E) embodies the principle that for two things (y and z) to be equivalent it suffices that they compare equivalently with actual objects (those in the range of the *bound* variable x). The axiom ($\forall$) of *universal instantiation* permits the passage from a bound variable statement to the corresponding free variable statement *given* the premise of *existence*. The axiom of *descriptions* (I) requires the outer quantifier: an *existing* element is equivalent to the element described just in case it is the only (existing) element satisfying the predicate. We need not mention improper descriptions explicitly, their properties follow from the axiom of extensionality and the properties of the quantifier. The *first-order* axioms stop here. (Of course if we were *just* doing first-order logic we would add the other connectives, the existential quantifier and the “obvious” axioms and rules — those of Theorem 3.5.)

To axiomatize the higher-order logic we add the full comprehension axiom (Comp): every predicate has an *extension*, a unique element of the appropriate power sort. We note that this axiom implies a property of extensionality for power sorts (Lemma 3.6(6)). The last axiom (Pred) of *predication* is more or less a grammatical convention: if we predicate a relation of certain arguments then both it and all its arguments should exist.

The rules are straightforward: *modus ponens* (MP) and *substitution* (Sub) are as usual. The rule ($\forall^+$) of *universal generalization* is *stronger* than the usual one since the premise is weakened by the existence assumption.

The notion of *derivability* is defined as usual. We write $\Gamma \vdash \varphi$ to mean that φ is derivable from the set Γ of formulae. A *theory* is a set T of formulae such that if $T \vdash \varphi$, then $\varphi \in T$. Any theory T is necessarily formulated in a language $L(T)$. We shall have occasion to use varying languages from time to time.

In the interests of readability we may write

$$\forall x : A. \varphi \quad \text{for } \forall x \varphi,$$

$$\exists x : A. \varphi \quad \text{for } \exists x \varphi,$$

where $\#x = A$, to make the implicit sort visible. We may also write $x : A$ to express that $\#x = A$.

3.4. DEFINITION. Taking advantage of quantification over “truth-values” we introduce the remainder of the traditional panoply of logical connectives by the following abbreviations:

- (1) $\varphi \vee \psi$ for $\forall z : [] (((\varphi \rightarrow z()) \wedge (\psi \rightarrow z())) \rightarrow z())$,
- (2) $\neg \varphi$ for $\forall z : [] (\varphi \rightarrow z())$,
- (3) $\exists x \varphi$ for $\forall z : [] (\forall x (\varphi \rightarrow z()) \rightarrow z())$,
- (4) $\top$ for $\mathbf{E}!y : [] . y()$,
- (5) $\perp$ for $\forall z : [] . z()$.

It is a simple exercise in finding formal derivations to show that these defined notions behave properly. The axiom and rule for the existential quantifier have to be modified to take account of existence (as with $\forall$).

3.5. THEOREM.

- (1) $\vdash \varphi \rightarrow \varphi \vee \psi$,
- (2) $\vdash \psi \rightarrow \varphi \vee \psi$,
- (3) $\vdash (\varphi \rightarrow \psi) \rightarrow ((\theta \rightarrow \psi) \rightarrow ((\varphi \vee \theta) \rightarrow \psi))$,
- (4) $\vdash (\varphi \rightarrow \psi) \rightarrow ((\varphi \rightarrow \neg \psi) \rightarrow \neg \varphi)$,
- (5) $\vdash \neg \varphi \rightarrow (\varphi \rightarrow \psi)$,
- (6) $\vdash \varphi \wedge \mathbf{E}x \rightarrow \exists x \varphi$,
- (7) $\vdash \top$,
- (8) $\vdash \perp \rightarrow \varphi$,
- (9) The rule $\frac{\varphi \wedge \mathbf{E}x \rightarrow \psi}{\exists x \varphi \rightarrow \psi}$ is valid where x is not free in ψ .

3.6. LEMMA.

- (1) $\vdash \mathbf{E}x \leftrightarrow \exists y . x = y$,
- (2) $\vdash \mathbf{E}!x \varphi \leftrightarrow \exists y \forall x (\varphi \leftrightarrow x = y)$,
- (3) $\vdash z \equiv !x \varphi \leftrightarrow \forall y (y \equiv z \leftrightarrow \forall x (x \equiv y \leftrightarrow \varphi))$,
- (4) $\vdash z(\dots, !x \varphi, \dots) \leftrightarrow \exists y (z(\dots, y, \dots) \wedge \forall x (\varphi \leftrightarrow x \equiv y))$,
- (5) $\vdash !x \varphi(\dots) \leftrightarrow \exists y (y(\dots) \wedge \forall x (\varphi \leftrightarrow x \equiv y))$,
- (6) $\vdash \forall y, z : [A_0, \dots, A_{n-1}] (y = z \leftrightarrow \forall \bar{x} (y(\bar{x}) \leftrightarrow z(\bar{x})))$,
- (7) $\vdash x \equiv y \leftrightarrow \forall z : [A] (z(x) \leftrightarrow z(y))$,
- (8) $\vdash \forall x, y (x \equiv y \leftrightarrow x = y)$,
- (9) $\vdash \mathbf{E}!x \varphi \rightarrow \varphi[!x \varphi / x]$.

These logical truths indicate how existence, descriptions, equivalence and equality are related. As a consequence we have the following labour-saving lemma remarked by Scott:

3.7. LEMMA. *Every formula φ of higher-order logic is logically equivalent to a description-free one.*

PROOF. By induction on the structure of φ using (2)–(5) of 3.6 to eliminate descriptions from atomic formulae. $\square$

The sorts given *ab initio* may be rather special and supply only a selection of the domains generally required in mathematics. However their higher-order structure makes them rich in subdomains. We define these more general (and more useful) *types* to be certain *syntactic* objects of our languages.

3.8. DEFINITION. A *type* $\mathbf{A}$ is a term of the syntactic form $\mathbf{I}y : [A]. \mathbf{A} (\varphi \leftrightarrow y(x))$ (which we abbreviate as $\{x : A \mid \varphi\}$). We say $\mathbf{A}$ is *definable* iff it is a closed term.

Each type $\mathbf{A} = \{x : A \mid \varphi\}$ is to be regarded as determining a subdomain of the sort A . (We could not define a type to be *any* term of sort $[A]$ since for different A, B it might occur that $[A] = [B]$, and so the term alone does not determine the underlying sort. However given any term τ of sort $[A]$ there is an obvious associated type $\{x : A \mid \tau(x)\}$.) For $\mathbf{A} = \{x : A \mid \varphi\}$ we use the notations $\tau \in \mathbf{A}$; $\forall x \in \mathbf{A}$; $\exists x \in \mathbf{A}$ with their obvious meanings, where τ and x are of sort A .

3.9. DEFINITION. A (*definable*) *relation* $\mathbf{F}$ from A to B is a (closed) term of the form

$$\mathbf{I}z : [A, B]. \forall x : A, y : B (z(x, y) \leftrightarrow \varphi).$$

(Again the syntactical form of $\mathbf{F}$ carries with it information on A and B .) We do not need to know that a relation $\mathbf{F}$ from A to B is (the graph of) a partial function to employ the ordinary *function-value notation*

$$\mathbf{F}'(\tau) \quad \text{for } \mathbf{I}y : B. \mathbf{F}(\tau, y),$$

where τ is a term of sort A . If σ is a term of sort B and $x : A$ we define *functional abstraction* by abbreviation, writing

$$\lambda x : A. \sigma \quad \text{for } \mathbf{I}z : [A, B]. \forall x, y [z(x, y) \leftrightarrow y = \sigma].$$

3.10. LEMMA. *The usual conversion principles hold:*

- (1) $\vdash \forall x : A (x \in \{x : A \mid \varphi\} \leftrightarrow \varphi),$
- (2) $\vdash \forall x : A ((\lambda x : A. \sigma)'(x) \equiv \sigma).$

4. Categories from logic

Our eventual aim is to show how topoi correspond to *theories* in our logic. Here we look at some categories arising from such theories and examine their structure in terms of the concepts introduced in Section 2. To construct a category from a theory T we take as objects a collection of *definable types* and as morphisms take the *definable total functions* between these types. The idea of constructing such *syntactic categories* (due to A. Joyal) has been exploited by REYES [1975] and others.

4.1. DEFINITION. The category $\mathbb{C}(T)$ of *sorts and definable total functions* of T has as *objects* the sorts of $L(T)$ and as *morphisms* from A to B equivalence classes of definable relations F from A to B such that

$$T \vdash \forall x : A. \mathbf{E}F'(x),$$

where F and G are equivalent iff

$$T \vdash \forall x : A (F'(x) \equiv G'(x)).$$

The composition $F \circ G$ is given (when it is defined) by the term

$$\lambda x. F'(G'(x)).$$

Checking that $\mathbb{C}(T)$ is a category is easy. We leave it to the reader. In general, the following construction gives a more interesting category.

4.2. DEFINITION. The category $\mathbb{E}(T)$ of *definable types and definable total functions* of T has the definable types of $L(T)$ as *objects* and as *morphisms* from A to B equivalence classes of definable relations F from A to B such that

$$T \vdash \forall x \in A. F'(x) \in B,$$

where F and G are equivalent iff

$$T \vdash \forall x \in A. F'(x) \equiv G'(x).$$

The composition of F and G is defined as in the previous definition.

Again it is simple to see that we have a category. The following lemmas examine its structure. The proofs are just syntactic versions of the proof that the classical category **Sets** has the corresponding structure. We sketch the necessary constructions leaving the details to the reader.

4.3. LEMMA. $\mathbf{E}(T)$ has finite products.

PROOF. $\{z : [] \mid z()\}$ acts as a terminal object since

$$\vdash \mathbf{E}!y. y \in \{z : [] \mid z()\}.$$

If $\tau : A$ and $\sigma : B$ we write $\langle \tau, \sigma \rangle$ for

$$\lambda z : [A, B]. \forall x, y (z(x, y) \leftrightarrow x = \tau \wedge \sigma = y).$$

The product $A \times B$ is given by

$$\{z : [A, B] \mid \exists x \in A, y \in B. z = \langle x, y \rangle\}$$

with the projections exemplified by

$$\lambda z. \lambda x. \exists y. z = \langle x, y \rangle$$

from $A \times B$ to A . $\square$

In future we shall write $\lambda(x, y). \tau$ for

$$\lambda z. \lambda w. \exists x, y (z = \langle x, y \rangle \wedge \tau = w).$$

4.4. LEMMA. $\mathbf{E}(T)$ has finite limits.

PROOF. Let $F, G : A \rightarrow B$ in $\mathbf{E}(T)$. The equalizer of F and G has as its domain

$$\{x : A \mid x \in A \wedge F'(x) = G'(x)\}$$

and is represented by $\lambda x. x$. $\square$

4.5. LEMMA. $\mathbf{E}(T)$ is Cartesian closed.

PROOF. The exponent B^A is given by

$$\{z : [A, B] \mid \forall x \in A. \mathbf{E}!y \in B. z(x, y) \wedge \forall x, y (z(x, y) \rightarrow x \in A \wedge y \in B)\}$$

with the evaluation morphism given by

$$\lambda(x, z). \lambda y. z(x, y).$$

For $F : A \times X \rightarrow B$ the morphism $\hat{F} : X \rightarrow B^A$ is given by

$$\lambda w. \lambda z : [A, B]. \forall x, y (z(x, y) \leftrightarrow y = F'(\langle x, w \rangle)). \quad \square$$

4.6. LEMMA. *A morphism $F : A \rightarrow B$ in $\mathbf{E}(T)$ is a monomorphism iff*

$$T \vdash \forall x, y \in A (F'(x) = F'(y) \rightarrow x = y).$$

PROOF. Let F be a monomorphism. We have two morphisms

$$G = \lambda(x, y). x \quad \text{and} \quad H = \lambda(x, y). y$$

(the projections) from

$$E = \{z : [A, A] \mid \exists x, y \in A (z = \langle x, y \rangle \wedge F'(x) = F'(y))\}$$

to A . It is easy to see that $F \circ G = F \circ H$ hence as F is monic $G = H$. That is to say,

$$T \vdash \forall z \in E (G'(z) = H'(z))$$

whence

$$T \vdash \forall x, y \in A (F'(x) = F'(y) \rightarrow x = y).$$

The proof in the other direction is easier still $\square$

4.7. LEMMA. *A commuting square in $\mathbf{E}(T)$*

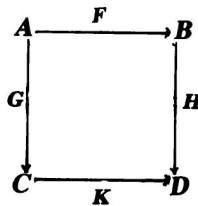


Diagram 5.

is a pullback iff

$$T \vdash \forall x \in B, y \in C (H'(x) = K'(y) \rightarrow \exists! z \in A (F'(z) = x \wedge G'(z) = y)).$$

PROOF. The proof one way is straightforward, from the formula we can deduce the pullback property. Now let K and H be as above. Consider the diagram

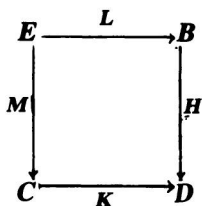


Diagram 6.

where L and M are the “projections” of

$$E = \{z : [B, C] \mid \exists x \in B. y \in C (z = \langle x, y \rangle \wedge H'(x) = K'(y))\}.$$

This is a pullback (using the easy direction of the lemma). The result now follows from the uniqueness of pullbacks up to isomorphism. $\square$

5. Topoi

Here we introduce elementary topoi and give some examples. In particular we show that for any theory T the category $\mathbb{E}(T)$ is a topos. We shall see in Section 7 that every topos is of this form.

5.1. DEFINITION. A *topos* is a Cartesian-closed category with a subobject classifier.

To understand this we need:

5.2. DEFINITION. A *subobject classifier* is a morphism $\text{true} : 1 \rightarrow \Omega$ (this distinguishes the codomain and an important “element”) such that pullbacks along true exist and for any mono $m : A' \rightarrowtail A$ there is a unique morphism $\text{cl}(m)$ (the *classifier* of m) making the diagram a pullback.

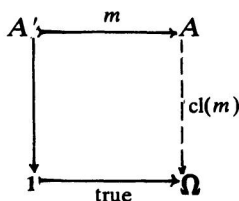


Diagram 7

Ω is to be thought of as a type of “truth values”. It is immediate from the definition that in a topos the set $\mathcal{P}(A)$ of subobjects of an object A is in

1-1 correspondence with the set $\text{Hom}(A, \Omega)$ of morphisms from A to Ω . To determine a function whose values are truth values, it suffices to determine the subobject on which it takes the value true. We shall often need to refer to the morphism $\text{true}_A : A \rightarrow \Omega$ which is given by composing $\text{true} : 1 \rightarrow \Omega$ with the (unique) morphism from A to 1 . A morphism $f : A \rightarrow \Omega$ factors through true iff $f = \text{true}_A$. A subobject classifier if it exists is unique up to a unique isomorphism.

5.3. THEOREM. *The category $\mathbb{E}(T)$ is a topos.*

PROOF. The subobject classifier is given by taking as Ω the object

$$\{x : [] \mid T\}$$

true being the morphism given by

$$\lambda x. \text{!}y : [] y().$$

For a monomorphism $M : A' \rightarrowtail A$ we take

$$\lambda x. \text{!}y : [] (y() \leftrightarrow \exists z \in A'. x = M'(z)).$$

Using the characterization of Lemma 4.7 it is easily seen that this gives a pullback and is unique with the property. Since we already know $\mathbb{E}(T)$ to be Cartesian closed with finite limits we are done. $\square$

Of course a similar syntactic construction may be used to produce a topos from a classical set theory.

Example. Let L be the first-order language of set theory, T a theory in L containing classical Zermelo set theory. The category of definable sets and functions of T is a topos. It has as objects formulae $\varphi(x)$ of L (we use parentheses to indicate a complete non-repetitive enumeration of the free variables of a formula) such that

$$T \vdash \exists y \forall x (\varphi(x) \leftrightarrow x \in y).$$

As morphisms from $\varphi(x)$ to $\psi(y)$ we take equivalence classes (under T -provable equivalence) of formulae $\theta(x, y)$ such that

$$T \vdash \forall x, y (\theta(x, y) \rightarrow \varphi(x) \wedge \psi(y)),$$

$$T \vdash \forall x (\varphi(x) \rightarrow \exists z \forall y (\theta(x, y) \leftrightarrow y = z)).$$

We leave the definition of composition to the reader. In this example the

algebra $\text{Hom}(1, \Omega)$ of definable elements of Ω is just the Lindenbaum algebra of T .

Before going on to develop some of the theory of topoi we introduce some more concrete examples.

5.4. DEFINITION. Let Ω be a complete Heyting algebra. An Ω -set A is a set A equipped with a "symmetric, transitive Ω -valued relation", that is a map

$$e : A \times A \rightarrow \Omega$$

satisfying

$$e(a, b) = e(b, a), \quad e(a, b) \wedge e(b, c) \leq e(a, c)$$

for $a, b, c \in A$.

An Ω -set $A = (A, e)$ should be thought of as a Heyting-valued set with partial elements. The degree of equality of two elements is measured by e the degree of existence of a being given by $e(a, a)$. Ω -sets can be used to give a semantics for our logic (see FOURMAN and SCOTT [1977]). In fact it was with this model in mind that the logic was axiomatized.

5.5. DEFINITION. A *morphism of Ω -sets* from (A, e) to (B, f) is an extensional, total, single-valued Ω -relation, that is a map $g : A \times B \rightarrow \Omega$ satisfying

$$e(a, a') \wedge f(b, b') \wedge g(a, b) \leq g(a', b'),$$

$$e(a, a) = \bigvee_{b \in B} g(a, b),$$

$$g(a, b) \wedge g(a, b') \leq f(b, b')$$

for $a, a' \in A$ and $b, b' \in B$.

Example. The category of Ω -sets and their morphisms forms a topos, where the *composition* of $g : A \rightarrow B$ with $h : B \rightarrow C$ is given by

$$(h \circ g)(a, c) = \bigvee_{b \in B} (g(a, b) \wedge h(b, c)).$$

In the category of Ω -sets we have $\Omega = (\Omega, \leftrightarrow)$ where $\leftrightarrow$ is the bi-implication. In the case where Ω is the Heyting algebra $\mathcal{O}(X)$ of open sets of a topological space X , the category of Ω -sets is (equivalent to) the category $\text{Top}(X)$ of set-valued sheaves over X . Ω -sets have been described independently by HIGGS [1974] who (among other things) gives a proof of this equivalence.

More Examples. (i) The category of *finite sets* and arbitrary functions between them is a topos.

(ii) Let $\mathfrak{A} = (A, \varepsilon)$ be a model for Zermelo set theory. The category of *sets and functions of $\mathfrak{A}$* whose objects are the elements of A and whose morphisms from a to b are those f in A such that $\mathfrak{A} \models (f \text{ is a function from } a \text{ to } b)$ is a topos.

(iii) Let G be a group. The category of G -sets has as objects, sets equipped with a G -action and as morphisms functions preserving this action. It is a topos.

In these last three examples Ω is the set {true, false} (with the trivial action in the case of G -sets). The first two show the *lack* of axioms corresponding to the set-theoretical axioms of *infinity* and *replacement* in the definition of topoi. We shall discuss these axioms in Section 8.

Let G be the cyclic group of order 2 and consider the G -sets (a, e) and (b, f) where a is a singleton and e the trivial action, b is a two element set of f the non-trivial action. We think of (b, f) as having two elements (in the sense that the formula $\exists x, y. \neg x = y$ is satisfied) which the permutation makes indistinguishable thus preventing any of the functions from a to b being “definable”. There are no morphisms from (a, e) to (b, f) . In this way we apply the *syntactic* notion of definability to the category of G -sets, *a priori* a semantic entity.

6. Logical constructs in topoi

Here we develop that part of topos theory we shall need. This theory is due to LAWVERE and TIERNEY [1970]. The development is reminiscent of that of algebraic logic. The Cartesian-closed structure gives us certain “finite types” and encapsulates the fact that definable maps are closed under composition, λ -abstraction and pairing. The correspondence between the set $\mathcal{P}(A)$ of subobjects of A and $\text{Hom}(A, \Omega)$ allows for a fruitful interplay between the *algebraic properties* of the category and the *logical properties* of Ω .

6.1. DEFINITION. The *equality* morphism $=_A : A \times A \rightarrow \Omega$ classifies the *diagonal* $\Delta_A = \langle A, A \rangle : A \rightarrow A \times A$.

6.2. LEMMA. *Topoi are finitely complete.*

PROOF. It suffices to show that we have equalizers. Given $f, g : A \rightarrow B$, the subobject of A classified by $=_B \circ \langle f, g \rangle$ is easily seen to be their equalizer. $\square$

6.3. DEFINITION. We give the “truth table” definitions

$$\wedge : \Omega \times \Omega \rightarrow \Omega \quad \text{classifies} \quad \langle \text{true}, \text{true} \rangle : 1 \rightarrow \Omega \times \Omega$$

$$\leftrightarrow : \Omega \times \Omega \rightarrow \Omega \quad \text{classifies} \quad \langle \Omega, \Omega \rangle : \Omega \rightarrow \Omega \times \Omega$$

and extend these operations to each poset $\mathcal{P}(A)$ of subobjects of an object A . Confusing a subobject with the corresponding morphism $A \rightarrow \Omega$, let

$$a \wedge b := \wedge \circ \langle a, b \rangle,$$

$$a \leftrightarrow b := \leftrightarrow \circ \langle a, b \rangle,$$

and

$$a \rightarrow b := (a \wedge b) \leftrightarrow a.$$

In a topos we can represent the subobject poset $\mathcal{P}(A)$ as a family of *sets* in a natural way. This will enable us to get a better hold on the operations we have just defined.

6.4. DEFINITION. To each subobject a of A we associate the *set* $\llbracket a \rrbracket$ of morphisms with codomain A which factor through a . Equivalently, identifying a with the corresponding morphism $a : A \rightarrow \Omega$ we write

$$\llbracket a \rrbracket = \{x : X \rightarrow A \mid a \circ x = \text{true}_X\}.$$

- 6.5. LEMMA.** (1) $a \leq b$ iff $\llbracket a \rrbracket \subseteq \llbracket b \rrbracket$;
 (2) $x \in \llbracket a \wedge b \rrbracket$ iff $x \in \llbracket a \rrbracket$ and $x \in \llbracket b \rrbracket$;
 (3) $c \leq a \wedge b$ iff $c \leq a$ and $c \leq b$;
 (4) $x \in \llbracket a \leftrightarrow b \rrbracket$ iff for all y , $x \circ y \in \llbracket a \rrbracket$ iff $x \circ y \in \llbracket b \rrbracket$;
 (5) $x \in \llbracket a \rightarrow b \rrbracket$ iff for all y , if $x \circ y \in \llbracket a \rrbracket$, then $x \circ y \in \llbracket b \rrbracket$;
 (6) $c \leq a \rightarrow b$ iff $c \wedge a \leq b$.

PROOF. These are all quite straightforward. For $\leftrightarrow$ note that

$$x \in \llbracket a \leftrightarrow b \rrbracket \quad \text{iff} \quad \langle a, b \rangle \circ x \text{ factors through } \langle \Omega, \Omega \rangle$$

$$\text{iff } a \circ x = b \circ x$$

$$\text{iff } \llbracket a \circ x \rrbracket = \llbracket b \circ x \rrbracket$$

but as $y \in \llbracket a \circ x \rrbracket$ iff $x \circ y \in \llbracket a \rrbracket$ we are done. $\square$

In showing that topoi have equalizers we constructed a subobject of A

by using the “internal logic” to describe those elements which should be in it. We shall use this idea again.

6.6. DEFINITION. Given $a \in \mathcal{P}(A \times B)$ we have a morphism $\hat{a} : B \rightarrow \Omega^A$. We also have $\hat{t} : B \rightarrow \Omega^A$ the transpose of $t : A \times B \rightarrow 1 \xrightarrow{\text{true}} \Omega$. We define $\Pi A(a)$ to be the subobject of B classified by

$$=_{\Omega^A} \circ \langle \hat{a}, \hat{t} \rangle.$$

Here we think of $\hat{a}$ as taking each x in B to the set of y in A such that $\langle y, x \rangle$ is in a and $\hat{t}$ as taking each x in B to A . $\Pi A(a)$ is to be thought of as the set of those x in B such that for all y in A the pair $\langle y, x \rangle$ is in a . As yet of course we can only make such thoughts precise when talking of topoi which we know to be of the form $\mathbf{E}(T)$. They are however invaluable to the intuition.

6.7. LEMMA. $x \in \llbracket \Pi A(a) \rrbracket$ iff $A \times x \in \llbracket a \rrbracket$.

PROOF. $x \in \llbracket \Pi A(a) \rrbracket$ iff $\hat{a} \circ x = \hat{t} \circ x$ iff $a \circ A \times x = t \circ A \times x$ iff $A \times x \in \llbracket a \rrbracket$. $\square$

Since the morphisms in a topos correspond to *total* maps they give us no direct information about *partial* elements. To interpret statements about partial elements in a topos we must use the higher-order structure to represent each object A as a subobject of some $\tilde{A}$ thought of as the domain of potential elements of A . In a topos $\mathbf{E}(T)$ we can construct such a domain letting $\tilde{A}$ be

$$\{x : [A] \mid \forall y, z : A ((x(y) \wedge x(z)) \rightarrow (y = z \wedge y \in A))\}$$

with the embedding of A given by $\lambda x. \{z : A \mid x = z\}$. This representation has the important property that predicates on A are in 1-1 correspondence with subdomains of $\tilde{A}$ since $\vdash x = y \leftrightarrow \{z : A \mid z = x\} = \{z : A \mid z = y\}$. The rest of this section is devoted to generalizing this construction to arbitrary topoi and examining its categorical properties.

6.8. DEFINITION. We write $\{\cdot\}_B$ for $=_{\hat{B}} : B \rightarrow \Omega^B$ and call it the *singleton morphism*. Now let $\xi : B \times \Omega^B \rightarrow \Omega$ classify $\langle B, \{\cdot\} \rangle : B \rightarrow B \times \Omega^B$ and take to be an equalizer.

$$\begin{array}{ccccc} \tilde{B} & \xrightarrow{e} & \Omega^B & \xrightarrow{\xi} & \Omega^B \\ & & & \searrow \Omega^B & \\ & & & & \end{array}$$

Diagram 8.

Since $B \times (\text{ev} \circ \{\cdot\} \circ f) = =_B \circ (B \times f)$ classifies $\langle f, X \rangle: X \rightarrow B \times X$, we see that f is recoverable from $\{\cdot\} \circ f$. Thus $\{\cdot\}$ is monic. Also $=_B$ and $\xi \circ (B \times \{\cdot\})$ are equal since they both classify the diagonal. Thus $\{\cdot\} = \hat{\xi} \circ \{\cdot\}$ and we have a factorization

$$\{\cdot\} = e \circ \eta,$$

where η is monic as $\{\cdot\}$ is. We call $\eta: B \rightarrow \tilde{B}$ a *partial map classifier* for B (see 6.12).

6.9. LEMMA. *The subobject $e: \tilde{B} \rightarrow \Omega^B$ is a retract (i.e. there is a morphism $r: \Omega^B \rightarrow \tilde{B}$ such that $r \circ e = \tilde{B}$).*

PROOF. Since $\hat{\xi} \circ \{\cdot\} = \{\cdot\}$ we have a pullback.

$$\begin{array}{ccc} B & \xrightarrow{\langle B, \{\cdot\} \rangle} & B \times \Omega^B \\ \downarrow & & \downarrow B \times \hat{\xi} \\ B & \xrightarrow{\langle B, \{\cdot\} \rangle} & B \times \Omega^B \end{array}$$

Diagram 9.

Thus $\xi \circ B \times \hat{\xi} = \xi$ (they classify the same subobject), hence $\hat{\xi} \circ \hat{\xi} = \hat{\xi}$ and we have a factorization

$$\hat{\xi} = e \circ r.$$

Now $e \circ \tilde{B} = e = \hat{\xi} \circ e = e \circ r \circ e$ and $\tilde{B} = r \circ e$ as e is monic. $\square$

6.10. LEMMA. *The projection $\pi: \tilde{B} \times X \rightarrow X$ is split (i.e. there is a morphism $s: X \rightarrow \tilde{B} \times X$ such that $\pi \circ s = X$).*

PROOF. It suffices to find a morphism from X to $\tilde{B}$ and pair it with the identity on X . Let $t = \text{true}_{B \times X}$ and let $s = \langle r \circ \hat{t}, X \rangle$. $\square$

This lemma expresses in a categorical way the fact that $\tilde{B}$ is inhabited.

6.11. DEFINITION. A *partial map* from A to B is a pair $(f, d): A \rightarrow B$ where $d: A' \rightarrow A$ is a subobject of A and $f: A' \rightarrow B$.

6.12. THEOREM. *Given a partial map $(f, d): A \rightarrow B$ there is a unique morphism $\tilde{f}: A \rightarrow B$ making the diagram a pullback. We say that $\tilde{f}$ classifies the partial map (f, d) .*

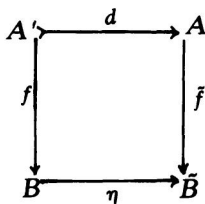


Diagram 10.

PROOF. Given a partial map $(f, d): A \rightarrow B$ we have a subobject $\langle f, d \rangle: A' \rightarrow B \times A$ called the graph of (f, d) . This is classified by a morphism $f^*: B \times A \rightarrow \Omega$. We show that $\hat{f}^*$ factors as $e \circ \tilde{f}: A \rightarrow \Omega^B$ and that $\tilde{f}$ has the desired properties.

If $\{\cdot\} \circ h = \hat{f}^* \circ g$, then $=_B \circ B \times h = f^* \circ B \times g$, so $=_B \circ \langle h, h \rangle = f^* \circ \langle h, g \rangle$. But $=_B \circ \langle h, h \rangle$ factors through *true* so $\langle h, g \rangle$ factors through $\langle f, d \rangle$. Since $\langle f, d \rangle$ is mono, this factorization is unique.

Also $=_B \circ B \times f = f^* \circ B \times d$ since they both classify (f, A') . We have shown that the square (i) is a pullback. Thus (ii) is a pullback so

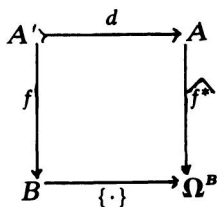


Diagram 11(i).

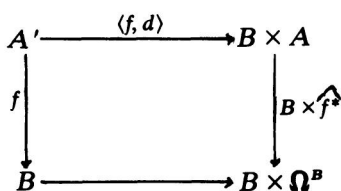


Diagram 11(ii).

$\xi \circ B \times \hat{f}^* = f^*$ since they both classify the same subobject. Hence $\hat{\xi} \circ \hat{f}^* = \hat{f}^*$ and we have a factorization

$$\hat{f}^* = e \circ \tilde{f}.$$

We obtain the diagram

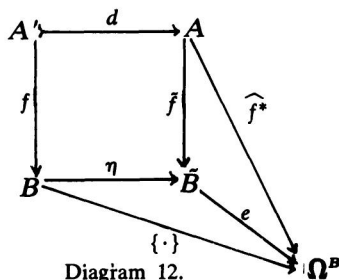


Diagram 12.

where the inner square commutes since e is monic and is a pullback since the outer one is.

Conversely, given such a diagram with the inner square a pullback, the square

$$\begin{array}{ccc}
 A' & \xrightarrow{\langle f, d \rangle} & B \times A \\
 f \downarrow & & \downarrow B \times \tilde{f} \\
 B & \xrightarrow{\langle B, \eta \rangle} & B \times \tilde{B}
 \end{array}$$

Diagram 13.

is a pullback.

Thus $\xi \circ B \times (e \circ \tilde{f}) = f^*$ (since they classify the same subobject). Hence $\hat{\xi} \circ e \circ \tilde{f} = \hat{f}^*$ and $\hat{\xi} \circ f = \hat{f}^*$. As e is monic, this tells us that $\tilde{f}$ is unique and we are done. $\square$

7. Interpretations in topoi

We extend our talk of “elements” of an object by showing how the logic of Section 3 may be interpreted in an arbitrary topos.

7.1. DEFINITION. Let $\mathbb{E}$ be a topos, L a language. An *interpretation* of L in $\mathbb{E}$ is a map $\mathcal{J}$ assigning to each sort A an object $\bar{A}$, to each constant c of sort A a morphism $[c]: 1 \rightarrow \bar{A}$ and to each finite sequence $(A_0, \dots, A_{n-1})$ of sorts an isomorphism

$$[\overline{A_0, \dots, A_{n-1}}] \cong \Omega^{x_{\bar{A}_i}}$$

By abuse of notation we write A for $\bar{A}$. We also suppose for simplicity that $[A_0, \dots, A_{n-1}] = \Omega^{x_{\bar{A}_i}}$: Strictly speaking the “canonical” isomorphisms given by the interpretation are necessary because of the abstract nature of the power-type map. Having realized this it is best, in the interests of clarity, to forget them.

7.2. DEFINITION. If Δ is a finite sequence of distinct variables of L we define an object $X\Delta$ of $\mathbb{E}$ by induction on the length of Δ

$$X(\) = 1, \quad X(\Delta, x) = X\Delta \times \tilde{A} \quad (\text{where } \#x = A).$$

Free variables are to range over potential elements, $X\Delta$ is to be thought of as the object of sequences of potential elements over which the sequence Δ shall range. If $\text{rng } \Delta \subseteq \text{rng } \Gamma$, then the product of projections gives a morphism

$$\pi_{\Delta}^{\Gamma} : X\Gamma \rightarrow X\Delta$$

which should be thought of as taking an n -tuple of partial elements of $X\Gamma$ to the corresponding m -tuple of partial elements of $X\Delta$. If $\Delta = (x_0, \dots, x_{n-1}, y)$, where $\#y = [\#x_0, \dots, \#x_{n-1}]$ there is a morphism

$$\text{ev} : X\#x_i \times \Omega^{\times \#x_i} \rightarrow \Omega$$

which classifies some subobject. Composing this subobject with the mono

$$X\eta : X\#x_i \times \Omega^{\times \#x_i} \rightarrow X\Delta$$

we get a subobject of $X\Delta$ whose classifier we denote by

$$\tilde{\text{ev}}_{\Delta} : X\Delta \rightarrow \Omega.$$

We shall also need the morphisms

$$\eta_x : A \times X(\Delta \setminus x) \rightarrow X\Delta \quad \text{where } \#x = A$$

given by taking $\eta_A \circ \pi$ in the x coordinate and the appropriate projection in each other one. These morphisms serve to restrict our attention to those x which exist and will be used in the interpretation of the variable binding operators.

Finally let $\mathbf{E}_A : \tilde{A} \rightarrow \Omega$ classify η_A .

7.3. DEFINITION. For φ a formula, τ a term and Δ a non-repetitive finite sequence of variables containing the free variables of φ and τ , we define the *valuations*

$$\llbracket \varphi \rrbracket_{\Delta} : X\Delta \rightarrow \Omega,$$

$$\llbracket \tau \rrbracket_{\Delta} : X\Delta \rightarrow \tilde{A} \quad (\text{where } \tau : A).$$

A formula is interpreted by a subobject of the domain of tuples of potential elements. A term is interpreted by the total map which to a tuple of potential elements assigns the appropriate potential element of A . The definition is by induction on structure according to the following schemata:

$$\llbracket c \rrbracket_{\Delta} = \llbracket c \rrbracket \circ \pi_{\langle \rangle}^{\Delta},$$

$$\llbracket x \rrbracket_{\Delta} = \pi_{\langle x \rangle}^{\Delta},$$

$$\llbracket \tau \equiv \sigma \rrbracket_{\Delta} = =_A \circ \langle \llbracket \tau \rrbracket_{\Delta}, \llbracket \sigma \rrbracket_{\Delta} \rangle,$$

$$\llbracket \mathbf{E}\tau \rrbracket_{\Delta} = \mathbf{E}_A \circ \llbracket \tau \rrbracket_{\Delta},$$

$$\llbracket \tau(\sigma_0, \dots, \sigma_{n-1}) \rrbracket_{\Delta} = \tilde{\mathbf{e}}\tilde{\mathbf{v}}_{\Delta} \circ \langle \llbracket \sigma_0 \rrbracket_{\Delta}, \dots, \llbracket \sigma_{n-1} \rrbracket_{\Delta}, \llbracket \tau \rrbracket_{\Delta} \rangle,$$

$$\llbracket \varphi \wedge \psi \rrbracket_{\Delta} = \wedge \circ \langle \llbracket \varphi \rrbracket_{\Delta}, \llbracket \psi \rrbracket_{\Delta} \rangle,$$

$$\llbracket \varphi \rightarrow \psi \rrbracket_{\Delta} = \rightarrow \circ \langle \llbracket \varphi \rrbracket_{\Delta}, \llbracket \psi \rrbracket_{\Delta} \rangle,$$

$$\llbracket \forall x. \varphi \rrbracket_{\Delta \setminus x} = \Pi A (\llbracket \varphi \rrbracket_{\Delta} \circ \eta_x).$$

To define $\llbracket 1x. \varphi \rrbracket_{\Delta \setminus x}$ given $\llbracket \varphi \rrbracket_{\Delta}$, let $\hat{\varphi} : X(\Delta \setminus x) \rightarrow \Omega^A$ be the transpose of $\llbracket \varphi \rrbracket_{\Delta} \circ \eta_x$. Pulling $\hat{\varphi}$ back along $\{ \cdot \}_A$ we get a partial map $X(\Delta \setminus x) \rightarrow A$. Let $\llbracket 1x. \varphi \rrbracket_{\Delta \setminus x}$ be the classifier of this partial map.

To supplement the last two clauses we must show how to define $\llbracket \psi \rrbracket_{\Delta}$ and $\llbracket \tau \rrbracket_{\Delta}$ from $\llbracket \psi \rrbracket_{\Delta \setminus x}$ and $\llbracket \tau \rrbracket_{\Delta \setminus x}$ where $x \notin \text{FV}(\psi)$, $\text{FV}(\tau)$. This is done by the schemata

$$\llbracket \varphi \rrbracket_{\Delta} = \llbracket \varphi \rrbracket_{\Gamma} \circ \pi_{\Gamma}^{\Delta}; \quad \llbracket \tau \rrbracket_{\Delta} = \llbracket \tau \rrbracket_{\Gamma} \circ \pi_{\Gamma}^{\Delta},$$

taking Γ to be $\Delta \setminus x$. Throughout this definition we have made the tacit assumption that $\#x = \#\tau = A$.

7.4. DEFINITION. The interpretation $\mathcal{I}$ satisfies φ (symbolically $\mathcal{I} \models \varphi$) iff whenever $\text{FV}(\varphi) \subseteq \text{rng } \Delta$ the morphism $\llbracket \varphi \rrbracket_{\Delta}$ factors through true. If $\mathbf{T}$ is a theory, we say $\mathcal{I}$ is a *model of T*, symbolically $\mathcal{I} \models T$, iff for all $\varphi \in T$ we have $\mathcal{I} \models \varphi$.

It follows from Lemma 6.10 that π_{Δ}^{Γ} is split, thus $\llbracket \varphi \rrbracket_{\Gamma}$ factors through true iff $\llbracket \varphi \rrbracket_{\Delta}$ does, where Δ is some enumeration of $\text{FV}(\varphi)$. It follows that $\mathcal{I} \models \varphi$ iff $\llbracket \varphi \rrbracket_{\Gamma}$ factors through true for some Γ with $\text{FV}(\varphi) \subseteq \text{rng } \Gamma$.

7.5. Definition. If τ is a term with $\text{FV}(\tau) \subseteq \text{rng } \Gamma$ and $\text{rng}(\Delta \setminus x) \subseteq \text{rng } \Gamma$ we define the morphism

$$[\tau/x]_{\Delta}^{\Gamma} : X\Gamma \rightarrow X\Delta$$

to be $\llbracket \tau \rrbracket_{\Gamma}$ in the x -coordinate and the appropriate projection in the others. If $x \notin \text{rng } \Delta$, then $[\tau/x]_{\Delta}^{\Gamma}$ is just π_{Δ}^{Γ} .

7.6. LEMMA.

$$\llbracket \sigma[\tau/x] \rrbracket_{\Gamma} = \llbracket \sigma \rrbracket_{\Delta} \circ [\tau/x]_{\Delta}^{\Gamma}, \quad \llbracket \varphi[\tau/x] \rrbracket_{\Gamma} = \llbracket \varphi \rrbracket_{\Delta} \circ [\tau/x]_{\Delta}^{\Gamma}.$$

PROOF. By induction on the structures of σ and φ . $\square$

7.7. LEMMA. Writing $\llbracket \varphi \rrbracket_{\Delta}$ for $\llbracket \llbracket \varphi \rrbracket_{\Delta} \rrbracket$ we have

$$\begin{aligned}\llbracket \varphi[\tau/x] \rrbracket_{\Gamma} &= \{f \mid [\tau/x]_{\Delta}^{\Gamma} \circ f \in \llbracket \varphi \rrbracket_{\Delta}\}, \\ \llbracket \mathbf{E}\tau \rrbracket_{\Delta} &= \{f \mid \llbracket \tau \rrbracket_{\Delta} \circ f \text{ factors through } \eta\}, \\ \llbracket \tau \equiv \sigma \rrbracket_{\Delta} &= \{f \mid \llbracket \tau \rrbracket_{\Delta} \circ f = \llbracket \sigma \rrbracket_{\Delta} \circ f\}, \\ \llbracket \varphi \wedge \psi \rrbracket_{\Delta} &= \llbracket \varphi \rrbracket_{\Delta} \cap \llbracket \psi \rrbracket_{\Delta}, \\ \llbracket \varphi \rightarrow \psi \rrbracket_{\Delta} &= \{f \mid \text{for all } g (f \circ g \in \llbracket \varphi \rrbracket_{\Delta} \Rightarrow f \circ g \in \llbracket \psi \rrbracket_{\Delta})\}, \\ \llbracket \forall x \varphi \rrbracket_{\Delta \setminus x} &= \{f \mid \eta_A \times f \in \llbracket \varphi \rrbracket_{\Delta}\}.\end{aligned}$$

PROOF. The first of these follows from the preceding lemma, the rest from Lemma 6.5 and the definition of valuation. $\square$

7.8. SOUNDNESS THEOREM (for interpretations in topoi). *If φ is an axiom, then $\mathcal{I} \models \varphi$; furthermore if $\mathcal{I}$ satisfies the premisses of a rule of inference, then it satisfies the conclusion.*

PROOF. The propositional axioms and $(\equiv)$ are easily checked using the preceding lemma as are the rules of substitution and *modus ponens*. We now check the remaining axioms and the introduction rule for the quantifier individually.

Axiom (E). For $f: Z \rightarrow \tilde{A} \times \tilde{A}$, we show that if

$$f \in \llbracket \forall z (z \equiv x \leftrightarrow z \equiv y) \rrbracket_{(x,y)},$$

then $\pi_1 \circ f$ and $\pi_2 \circ f$ classify the same partial map. By the uniqueness of partial map classifiers, this shows that they are equal and we are done.

Let f be as above and g be such that we have a factorization

$$\pi_2 \circ f \circ g = \eta_A \circ h.$$

It suffices by symmetry to show that

$$\pi_1 \circ f \circ g = \eta_A \circ h.$$

Now

$$\langle \pi_2 \circ f \circ g, f \circ g \rangle = (\eta_A \times f) \circ \langle h, g \rangle \in \llbracket z \equiv x \leftrightarrow z \equiv y \rrbracket_{(z,x,y)}.$$

But

$$\langle \pi_2 \circ f \circ g, f \circ g \rangle \in \llbracket z \equiv y \rrbracket_{(z,x,y)},$$

hence

$$\langle \pi_2 \circ f \circ g, f \circ g \rangle \in \llbracket z \equiv x \rrbracket_{(z, x, y)},$$

i.e.,

$$\pi_2 \circ f \circ g = \pi_1 \circ f \circ g.$$

Axiom (V), Rule (V⁺). We deal with the rule and the axiom together, by showing that if $x \notin \text{FV}(\varphi)$ then $\mathbf{E}x \wedge \varphi \rightarrow \psi$ is satisfied iff $\varphi \rightarrow \mathbf{V}x : A\psi$ is. Now

$$\begin{aligned} \llbracket \varphi \rrbracket_{\Delta \setminus x} \leq \llbracket \mathbf{V}x\psi \rrbracket_{\Delta \setminus x} = \Pi A (\llbracket \psi \rrbracket \circ \eta_x) \quad \text{iff} \quad \llbracket \varphi \rrbracket_{\Delta} \circ \eta_x \leq \llbracket \psi \rrbracket_{\Delta} \circ \eta_x \\ \text{iff} \quad \llbracket \varphi \wedge \mathbf{E}x \rrbracket \leq \llbracket \psi \rrbracket_{\Delta}. \end{aligned}$$

Since $\varphi \rightarrow \psi$ is satisfied iff $\llbracket \varphi \rrbracket_{\Delta} \leq \llbracket \psi \rrbracket_{\Delta}$ we are done.

Axiom (I). We must show that for all $f : X \rightarrow X\Delta$ we have

$$\eta_A \times f \in \llbracket y \equiv \mathbf{I}x \leftrightarrow \mathbf{V}x (\varphi \leftrightarrow x \equiv y) \rrbracket_{y, \Delta}.$$

From the definition of $\llbracket \mathbf{I}x\varphi \rrbracket$ we see that for $h : Y \rightarrow A \times X\Delta$,

$$\eta_A \circ \pi \circ h = \llbracket \mathbf{I}x\varphi \rrbracket \circ \eta_A \times X\Delta \circ h$$

if

$$= {}_A \circ \pi_{12} \circ A \times h = \llbracket \varphi \rrbracket \circ \eta_A \times \eta_A \times X\Delta \circ A \times h.$$

Thus for all $g : Y \rightarrow A \times X$ we have

$$\eta_A \times f \circ g \in \llbracket y \equiv \mathbf{I}x\varphi \rrbracket_{y, \Delta}$$

iff

$$\eta_A \times f \circ g \in \llbracket \mathbf{V}x (\varphi \leftrightarrow x \equiv y) \rrbracket_{y, \Delta}$$

$$(\text{as } =_{\bar{A}} \circ \eta_A \times \eta_A = =_A).$$

Axiom (Comp). It suffices to show that $\llbracket \mathbf{I}y \mathbf{V}\bar{x} (\varphi \leftrightarrow y(\bar{x})) \rrbracket$ factors through η . We show that

$$\llbracket \mathbf{I}y \mathbf{V}\bar{x} (\varphi \leftrightarrow y(\bar{x})) \rrbracket = \eta \circ \hat{\varphi},$$

where $\hat{\varphi}$ is the transpose of $\llbracket \varphi \rrbracket_{\bar{x}, \Delta} \circ X\eta \times X\Delta$. For this it is enough to show that

$$=_{\Omega^{X_A} \circ \Omega^{X_A} \times \hat{\varphi}} \llbracket \mathbf{V}\bar{x} (\varphi \leftrightarrow y(\bar{x})) \rrbracket \circ \eta_y.$$

Now since $\text{ev} \circ X\eta \times \eta = \text{ev}$, we have

$$f \in \llbracket \mathbf{V}\bar{x} (\varphi \leftrightarrow y(\bar{x})) \rrbracket_{y, \Delta} \circ \eta_y \rrbracket$$

iff

$$\llbracket \varphi \rrbracket_{\bar{x}, \Delta} \circ X\eta \times (\pi_2 \circ f) = \text{ev} \circ XA_i \times (\pi_1 \circ f)$$

iff

$$\hat{\varphi} \circ \pi_2 \circ f = \pi_1 \circ f$$

iff

$$f \in \llbracket =_{\Omega^{\mathbf{X}A'} \circ \Omega^{\mathbf{X}A_i} \times \hat{\varphi}} \rrbracket.$$

Axiom (Pred). This is immediate from the definition of $\tilde{e}\tilde{v}$.

7.9. DEFINITION. To each interpretation we associate a theory

$$T(\mathcal{J}) = \{\varphi \mid \mathcal{J} \models \varphi\}.$$

For any theory $\mathbf{T}$ the *canonical* interpretation $\mathcal{J}(\mathbf{T})$ of $\mathbf{T}$ in $\mathbf{E}(\mathbf{T})$ is defined by interpreting $\mathbf{L}(\mathbf{T})$ in $\mathbf{E}(\mathbf{T})$ as follows: Each sort A is interpreted by the type $\bar{A} = \{x : A \mid x = x\}$. If c is a constant of sort A in $\mathbf{L}(\mathbf{T})$ we have a morphism

$$\lambda z : [\] . c : \{z : [\] \mid z(\) \wedge \mathbf{E}c\} \rightarrow \bar{A}$$

defined on a subobject of $\mathbf{1}$. We let

$$\llbracket c \rrbracket : \mathbf{1} \rightarrow \bar{A}$$

be its classifier.

7.10. THEOREM. $\mathcal{J}(\mathbf{T}) \models \varphi$ iff $\mathbf{T} \vdash \varphi$.

PROOF (outline). Since every formula is logically equivalent to a description-free formula and our interpretations are sound it suffices to consider description-free φ . The result follows from the fact that for such φ the morphism

$$\llbracket \varphi \rrbracket_{\Delta} : \mathbf{X}\Delta \rightarrow \Omega$$

is just

$$\lambda x_0, \dots, x_{n-1} \lambda y : [\] (y(\) \leftrightarrow \varphi(\llbracket z x_0(z), \dots, \llbracket z x_{n-1}(z) \rrbracket))$$

which is proved by a tedious induction on the structure of φ . $\square$

7.11. COROLLARY. *Our axiomatization of the logic of partial elements is complete for interpretations in topoi.*

For a proof of a completeness theorem for our logic along more traditional lines see FOURMAN and SCOTT [1977]. Let $\mathcal{J}$ now be an interpretation of $\mathbf{L}$ in $\mathbf{E}$. For A a definable type we extend the abuse which identifies a sort A with the object interpreting it by writing A for the

subobject of $\tilde{A}$ classified by $\llbracket x \in A \rrbracket$. Since $\vdash x \in A \rightarrow \mathbf{E}x$ we have a factorization of the inclusion $\gamma_A = \eta_A \circ i_A : A \rightarrow \tilde{A}$.

7.12. LEMMA. *If A and B are definable types and F is a definable relation from A to B , then*

$$\mathcal{J} \models \forall x \in A. F'(x) \in B$$

iff there is a morphism $f : A \rightarrow B$ in $\mathbf{E}$ such that either of the following (equivalent) diagrams commutes.

$$\begin{array}{ccc} A \times B & \xrightarrow{\gamma \times \gamma} & \tilde{A} \times \tilde{B} \\ \downarrow f \times B & & \downarrow \llbracket F(x, y) \rrbracket \\ B \times B & \xrightarrow{=_{\mathbf{B}}} & \Omega \end{array} \quad \begin{array}{ccc} A & \xrightarrow{\gamma_A} & \tilde{A} \\ \downarrow f & & \downarrow \llbracket F'(x) \rrbracket \\ B & \xrightarrow{\gamma_B} & \tilde{B} \end{array}$$

Diagram 14.

In this case f is uniquely determined by F . Two such relations F and G determine the same morphism iff

$$\mathcal{J} \models \forall x \in A. F'(x) = G'(x).$$

PROOF. $\models \forall x \in A. F'(x) \in B$ iff $\llbracket F'(x) \rrbracket \circ \gamma_A$ factors as $\gamma_B \circ f$ (f is then uniquely determined as γ is monic) iff

$$(F(x, y))^{\wedge} \circ \gamma_A = \{ \cdot \}_B \circ i_B \circ f$$

(see definition of $\llbracket \mathbf{I}x. \varphi \rrbracket$ on p. 1078) iff

$$\llbracket F(x, y) \rrbracket \circ \eta_B \times \gamma_A = =_B \circ B \times (i_B \circ f)$$

iff

$$\llbracket F(x, y) \rrbracket \circ \gamma_B \times \gamma_A = =_B \circ B \times f.$$

The last part is obvious from the fact that

$$\models \forall x \in A, y \in B. (F(x, y) \leftrightarrow G(x, y))$$

iff

$$\llbracket F(x, y) \rrbracket \circ \gamma_B \times \gamma_A = \llbracket G(x, y) \rrbracket \circ \gamma_B \times \gamma_A. \quad \square$$

Let $\mathcal{J}$ be an interpretation of $\mathbf{L}$ in $\mathbf{E}$. If F is a definable relation from A to B such that $\mathcal{J} \models \forall x \in A. F'(x) \in B$ we shall as a temporary (and most abusive) notation write F for the corresponding morphism from A to B in $\mathbf{E}$ (taking care that there can be no confusion as to the intended domain and codomain).

- 7.13. THEOREM.** (1) $F \circ G = H$ in $\mathbb{E}$ iff $\mathcal{J} \models \forall x \in A (F'(G'(x)) = H'(x))$.
 (2) A is a terminal object in $\mathbb{E}$ iff $\mathcal{J} \models \forall x, y \in A. x = y$.
 (3) $A \xleftarrow{P} C \xrightarrow{Q} B$ is a product in $\mathbb{E}$ iff

$$(4) \quad \mathcal{J} \models \forall x \in A, \quad \forall y \in B. \exists! z \in C (P'(z) = x \wedge Q'(z) = y).$$

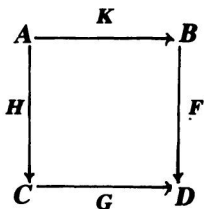


Diagram 15.

is a pullback in $\mathbb{E}$ iff it commutes and

$$\mathcal{J} \models \forall x \in B, y \in C (F'(x) = G'(y) \rightarrow \exists! z \in A (K'(z) = x \wedge H'(z) = y)).$$

- (5) $EV : A \times X \rightarrow B$ is an exponent in $\mathbb{E}$ iff

$$\mathcal{J} \models \forall z : [A, B] (\forall x \in A, \exists! y \in B. z(x, y) \rightarrow \exists! w \in X. \forall x \in A, y \in B (z(x, y) \leftrightarrow EV(x, w) = y)).$$

- (6) $T : 1 \rightarrow X$ is a subobject classifier in $\mathbb{E}$ iff

$$\mathcal{J} \models \forall x : [\quad]. \exists! y \in X (y = T'(*) \leftrightarrow x(\quad)),$$

where $*$ is the term $!z : 1. z = z$.

PROOF. Straightforward using the methods of Section 4. $\square$

8. Topoi as theories

8.1. DEFINITION. If $\mathbb{E}$ is a topos $L(\mathbb{E})$, the language of $\mathbb{E}$ has as sorts the objects of $\mathbb{E}$ and as constants of sort A the pairs (c, A) where $c : 1 \rightarrow \tilde{A}$. The power-type map is given by

$$[A_0, \dots, A_{n-1}] = \Omega^{x_{A_i}}.$$

The canonical interpretation $I(\mathbb{E})$ of $L(\mathbb{E})$ in $\mathbb{E}$ is given by interpreting each sort by itself and letting $\llbracket (c, A) \rrbracket = c$. We may often write c for (c, A) where

confusion is unlikely. The *diagram* or *theory* of $\mathbb{E}$ is the set $T(\mathbb{E})$ of formulae of $L(\mathbb{E})$ satisfied by the canonical interpretation.

8.2. THEOREM. *If $\mathbb{F}$ is a topos $\mathbb{C}(T(\mathbb{F})) = \mathbb{F}$.*

PROOF. The objects of $\mathbb{C}(T(\mathbb{F}))$ are the sorts of $L(\mathbb{F})$ which in turn are the objects of $\mathbb{F}$. Each morphism $f : A \rightarrow B$ in $\mathbb{F}$ gives rise to a constant c of sort $[A, B]$ of $L(\mathbb{F})$ corresponding to the transpose of $=_B \circ B \times f$. By Lemma 7.12 the relation

$$f = \mathbf{I}z : [A, B]. \forall x : A, y : B (z(x, y) \leftrightarrow c(x, y))$$

represents a morphism of $\mathbb{C}(T(\mathbb{F}))$ and every such morphism arises from a unique morphism in $\mathbb{F}$. That composition in $\mathbb{C}(T(\mathbb{F}))$ corresponds to composition in $\mathbb{F}$ follows directly from Theorem 7.13(1). $\square$

We now consider the question of why $\mathbb{C}(T)$ is not in general a topos. This happens because it may lack objects.

8.3. DEFINITION. A theory T is *definitionally complete* iff for each definable type A there is a sort B , and definable relation F from B to A such that

$$T \vdash \forall x : B. \mathbf{E}F'(x),$$

$$T \vdash \forall x, y : B (F'(x) = F'(y) \rightarrow x = y),$$

$$T \vdash \forall z : A (\exists x : B. z = F'(x) \leftrightarrow z \in A).$$

8.4. LEMMA. *If $\mathbb{F}$ is a topos, $T(\mathbb{F})$ is definitionally complete.*

PROOF. Consider the canonical interpretation of $T(\mathbb{F})$ in $\mathbb{F}$. If A is a definable type the morphism

$$\llbracket x \in A \rrbracket \circ \eta : A \rightarrow \Omega$$

classifies a subobject of A which gives rise to the required sort and definable relation. $\square$

There is a canonical functor I (taking A to $\{x : A \mid \mathbf{E}x\}$) which embeds $\mathbb{C}(T)$ as a full subcategory of $\mathbb{E}(T)$.

8.5. THEOREM. *I is an equivalence of categories (every object in $\mathbb{E}(T)$ is isomorphic to one in the image of $\mathbb{C}(T)$) iff T is definitionally complete.*

PROOF. Immediate. $\square$

8.6. COROLLARY. *If T is definitionally complete $\mathbb{C}(T)$ is a topos.*

8.7. DEFINITION. A functor $H : \mathbb{E} \rightarrow \mathbb{F}$ between topoi is *logical* (a *morphism* of topoi) iff it preserves finite limits, exponents and subobject classifiers.

In logical terms, a logical functor may be pictured as an interpretation of one theory in another which is *standard* in that it interprets power-sorts by power-sorts.

If $H : \mathbb{E} \rightarrow \mathbb{F}$ is logical, then for any interpretation $\mathcal{J}$ of L in $\mathbb{E}$, the composite map $H \circ \mathcal{J}$ gives an interpretation of L in $\mathbb{F}$. (The necessary isomorphisms being given by the uniqueness up to a unique isomorphism of products exponents and subobject classifiers.)

8.8. LEMMA.

$$\llbracket \varphi \rrbracket_{H \circ \mathcal{J}} \cong H \llbracket \varphi \rrbracket_{\mathcal{J}},$$

$$\llbracket \tau \rrbracket_{H \circ \mathcal{J}} \cong H \llbracket \tau \rrbracket_{\mathcal{J}}.$$

PROOF. By induction on the structure of φ and τ . $\square$

8.9. THEOREM. *For any model $\mathcal{F}$ of a theory T in a topos $\mathbb{F}$ there is a logical functor $H : \mathbb{E}(T) \rightarrow \mathbb{F}$ unique up to a unique isomorphism such that $H \circ \mathcal{J}(T) = \mathcal{F}$.*

PROOF. Firstly we note that uniqueness up to isomorphism follows from the preceding lemma together with Lemma 7.12. Since $\mathcal{F}$ is a model of T , Lemma 7.12 tells us how to associate a morphism $f = H(F) : A \rightarrow B$ in $\mathbb{F}$ to a morphism $F : A \rightarrow B$ in $\mathbb{E}(T)$. That this map is in fact a logical functor follows from Theorem 7.13. $\square$

We see that topoi correspond to certain definitionally complete theories and logical morphisms correspond to interpretations which are models for these theories. Every theory T has a definitionally complete conservative extension — the theory associated to $\mathbb{E}(T)$. (In fact this extension is not only conservative, but also *inessential* in the sense that it has a natural interpretation in T : its expressive power is no greater than that of T .)

As remarked at the end of Section 5, the axioms for topoi contain no analogue of the set-theoretic axioms of *infinity* and *replacement*. The force

of the replacement axiom is to replace an unbounded quantifier by a restricted one. Since we have no categorical analogue of the unbounded quantifier the absence of replacement from the topos axioms is not surprising. A categorical version of an axiom of infinity (due to Lawvere) is given by demanding that there be a natural number object (NNO). We shall examine briefly which theories correspond to topoi with NNO.

8.10. DEFINITION. A *natural number object* is an object N equipped with morphisms $1 \xrightarrow{0} N \xrightarrow{s} N$ satisfying the recursion property: for any diagram $1 \xrightarrow{a} A \xrightarrow{f} A$ there is a unique morphism $k : N \rightarrow A$ such that $k \circ 0 = a$ and $f \circ k = k \circ s$.

8.11. THEOREM (HATCHER [1968], OSIUS [1975], Folklore). *An object N with the structure $1 \xrightarrow{0} N \xrightarrow{s} N$ is a NNO in the topos $\mathcal{E}$ iff the following formulae (Peano's Axioms) are satisfied by the canonical interpretation of $L(\mathcal{E})$ in $\mathcal{E}$:*

$$(P3) \quad \forall x : N. \neg 0 = s'(x),$$

$$(P4) \quad \forall x, y : N (s'(x) = s'(y) \rightarrow x = y),$$

$$(P5) \quad \forall X : [N] (0 \in X \wedge \forall x \in X. s'(x) \in X \rightarrow \forall x : N. x \in X).$$

A converse also holds:

8.12. THEOREM. *Let T be a theory in a language with a constant $0 : N$ and a definable relation s from N to N such that T proves the axioms P3–P5 of Theorem 8.11 and in addition*

$$(P1) \quad \mathbf{E}0,$$

$$(P2) \quad \forall x : N. \mathbf{E}s'(x).$$

then in $\mathcal{E}(T)$ we have a natural number object

$$1 \xrightarrow{0} N \xrightarrow{s} N.$$

We now consider briefly two applications:

8.13. THEOREM (Mikkelsen, PARÉ [1974]). *Topoi have finite colimits.*

PROOF. It suffices to consider topoi of the form $\mathcal{E}(T)$ since by Theorems 8.2 and 8.5 every topos is equivalent to one such. As in Section 4 we may now use straightforward logical constructions of colimits. It suffices to have an

initial object ($\{x : [] \mid \perp\}$), disjoint sums ($A + B$ may be constructed as a subtype of $[[A], [B]]$) and coequalizers (the coequalizer of F and $G : A \rightarrow B$) has as codomain a subtype of $[B]$). $\square$

Other categorical properties of topoi — exactness properties, the existence of a right adjoint to pulling back etc. — follow easily using this method. As a second application we consider the construction of free topoi. (In essence our method is the same as that of VOLGER [1975].)

8.14. DEFINITION. Let G be a directed graph (in the sense of MAC LANE [1971] p. 48). By a *condition* C on G we mean a statement in the expansion of the language of category theory having names for the nodes and paths of D . It is evident what it means for such a condition to be *satisfied* by a morphism from G to (the underlying graph of) a category C .

8.15. DEFINITION. The *language* $L(G)$ of a directed graph G is constructed as follows. The set of sorts of $L(G)$ is the least set of expressions containing the nodes of G and closed under the syntactic operation

$$(A_0, \dots, A_{n-1}) \mapsto [A_0, \dots, A_{n-1}]$$

(here we consider the nodes as formal symbols and the square brackets and commas as formal punctuation marks). For each edge $f : A \rightarrow B$ of G we have in $L(G)$ a constant f of sort $[A, B]$.

8.16. LEMMA. For $f : A \rightarrow B$ in G let $F = \lambda x. \lambda y : B. f(x, y)$ be the corresponding relation in $L(G)$. To any morphism F from G to a topos $\mathbb{E}$ there corresponds an interpretation $\mathcal{J}(F)$ of $L(G)$ in $\mathbb{E}$ such that for each $f : A \rightarrow B$ in G ,

$$\models \forall x : A. \mathbf{E}F'(x).$$

Conversely to any such interpretation there corresponds an essentially (up to isomorphism) unique morphism from G to $\mathbb{E}$.

8.17. DEFINITION. A condition C on G is said to be *internally expressible* iff there is a formula φ of $L(G)$ such that F satisfies C iff

$$\mathcal{J}(F) \models \varphi.$$

8.18. THEOREM. If G is a directed graph and $\mathcal{C}$ a set of internally expressible conditions on G , then there is a topos $\mathbb{F}$ and a morphism $F : G \rightarrow \mathbb{F}$ satisfying (the conditions in) $\mathcal{C}$, such that for every topos $\mathbb{E}$ and morphism $H : G \rightarrow \mathbb{E}$

satisfying $\mathcal{C}$ there is a logical functor $K : \mathbf{F} \rightarrow \mathbf{E}$ unique up to isomorphism such that $K \circ F = H$.

PROOF. The required topos is just $\mathbf{E}(T)$ where T is the theory in $\mathbf{L}(G)$ having as axioms

$$\forall x : A \ \mathbf{E}F'(x) \quad \text{for } f : A \rightarrow B \text{ in } \mathcal{G}$$

and for each $C \in \mathcal{C}$ the corresponding formula φ in $\mathbf{L}(G)$. $\square$

This theorem gives many free topoi since as we have seen many conditions are internally expressible. Here is a short list of such conditions: To be monic (epic, iso); to be a (co)product; to be a (co)equalizer; to be initial (terminal); to be a subobject classifier; to be an exponent; to be a pullback (pushout).

We hope in this chapter to have demonstrated (at least) two things: that categories are not as mysterious as they seem, and that topoi are not mysterious categories.

We have shown that in talking about some categories (topoi) we may talk concretely in terms of elements. This process may be extended to other categories by suitably embedding them in topoi. The lack of "elements" is no more mysterious than is a theory in which $\vdash \exists x \varphi(x)$ without there being a term τ such that $\vdash \varphi(\tau)$.

Topoi result if we apply intuitionistic logic (with partial elements) to the basic intuition of (finite) power types satisfying comprehension and extensionality. Other category theoretic abstractions may be viewed similarly: for example any abelian category may be represented as a full sub-abelian category of the category $\mathbf{Ab}(\mathbf{E})$ of abelian groups of some topos $\mathbf{E}$. Thus it may be viewed as a category of abelian groups in some appropriate logic.

To conclude we mention an embarrassment. The important morphisms between topoi are *geometric morphisms* (ARTIN, GROTHENDIECK and VERDIER [1972]). Our treatment does not explain this fact. REYES [1975] (see also Chapter A.8 of this volume) has shown how a Grothendieck topos may be viewed as the extension of Sets obtained by adding a generic model for a suitable (possibly infinitary) first-order theory T . Geometric morphisms then arise naturally from a consideration of models (in Grothendieck topoi) of such theories. This approach however depends on some fixed "base topos" (in this case Sets) and fails to explicate the notion of topos *in abstracto*.

References

- ARTIN, M., A. GROTHENDIECK and J.L. VERDIER, editors
 [1972] *Théorie des topos et cohomologie étale des schémas. Tôme 1*, Séminaire de Géométrie Algébrique du Bois-Marie 1963/64 (SGA 4) Lecture Notes in Mathematics, Vol. 269 (Springer, Berlin).
- BOILEAU, A.
 [1975] Types vs topos, Mimeo, Université de Montréal, Montréal, Canada.
- COSTE, M.
 [1974] Logique d'ordre supérieur dans les topos élémentaires, Mimeo, Seminaire Benabou, Paris.
- FOURMAN, M.P.
 [1974] Connections between category theory and logic, Ph.D. Thesis, Oxford.
- FOURMAN, M.P. and D.S. SCOTT
 [1977] Sheaves and logic, in: *Applications of Sheaves*, Proceedings of Durham Symposium, to appear.
- GRAY, J.W.
 [1971] The meeting of the Midwest Category Seminar in Zurich, in: *Reports of the Midwest Category Seminar V*, edited by J.W. Gray, Lecture Notes in Mathematics, Vol. 195 (Springer, Berlin) pp. 248–255.
- HATCHER, W.
 [1968] *The Foundations of Mathematics* (Saunders, Philadelphia, PA).
- HIGGS, D.
 [1974] A category approach to Boolean-valued set theory, preprint, Waterloo, to appear.
- LAWVERE, F.W.
 [1970] Quantifiers and sheaves, in: *Actes du Congrès International des Mathématiciens*, Tome 1, pp. 329–334.
 [1972] Introduction, in: *Toposes, Algebraic Geometry and Logic*, edited by F.W. Lawvere, Lecture Notes in Mathematics, Vol. 274 (Springer, Berlin) pp. 1–12.
 [1975] Introduction, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin) pp. 3–14.
- LAWVERE F.W. and M. TIERNEY
 [1970] Lectures on elementary topoi, Midwest Category Seminar, Zurich. (Summarized in GRAY [1971].)
- MAC LANE, S.
 [1971] *Categories for the Working Mathematician* (Springer, Berlin).
- OSIUS, G.
 [1975] Logical and set theoretical tools in elementary topoi, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin) pp. 297–346.
- PARÉ, R.
 [1974] Colimits in topoi, *Bull. Am. Math. Soc.*, **80** (3), 556–561.
- REYES, G.
 [1975] From sheaves to logic, in: *Studies in Algebraic Logic*, edited by A. Daigneault, M.A.A. Studies, Vol. 9 (Math. Assoc. Am., Buffalo, NY) pp. 143–204.
- ROUSSEAU, C.
 [1977] Complex analysis and topoi, *J. Pure and Appl. Algebra*, to appear.
- SCOTT, D.S.
 [1969] Boolean models and non-standard analysis, in: *Applications of Model Theory to Algebra Analysis and Probability*, edited by W.A.J. Luxemburg (Holt, Reinhart and Winston, NY) pp. 87–92.

- [1977] Identity and existence in intuitionistic logic, in: *Applications of Sheaves*, Proceedings of Durham Symposium, to appear.

TAKEUTI, G.

- [1977] Boolean-valued analysis, in: *Applications of Sheaves*, Proceedings of Durham Symposium, to appear.

VOLGER, H.

- [1975] Logical categories, semantical categories and topoi, in: *Model Theory and Topoi*, edited by F.W. Lawvere, C. Maurer and G.C. Wraith, Lecture Notes in Mathematics, Vol. 445 (Springer, Berlin) pp. 97–100.

*The Type Free Lambda Calculus**

HENK P. BARENDREGT**

Contents

0. Introduction . . .	1092
1. Towards the theory . . .	1094
2. Classical λ -calculus	1100
3. Construction of $\mathcal{P}\omega$	1106
4. Construction of D_∞	1110
5. Solvability . . .	1117
6. Böhm trees . . .	1119
7. Analysis of D_∞	1125
References	1131

* Part of the chapter was written while visiting the Forschungsinstitut für Mathematik, ETH, Zurich.

** The author wishes to thank Dana Scott for his basic remarks on a draft of this chapter, and Jane Bridge and Jeff Zucker for pointing out several errors in the text.

0. Introduction

The λ -calculus and its variable free equivalent, combinatory logic, were initiated around 1930 by Church, Schönfinkel and Curry respectively. The intention of the founders of the subject was to study *rules*; in other words to study the old-fashioned notion of “function” in the sense of *definition*. In contrast to Dirichlet’s notion (of *graph*, that is the set of pairs of argument and associated value) the older notion referred to the *process* of stepping from argument to value, a process coded by a definition. Generally we think of such definitions as given by words in ordinary English, applied to arguments also expressed by words (in English). Or, more specifically, we may think of the definitions as programs for machines applied to, that is, operating on, such programs. In both cases we have to do with a *type free* structure, where the objects of study are at the same time function and argument. In particular, a function can be applied to itself. For the usual conception of a function in mathematics (in Zermelo–Fraenkel set theory) this is impossible (because of the axiom of foundation).

The λ -calculus represents a class of (partial) functions (λ -definable functions) on the integers which turns out to be the class of (partial) recursive functions. The equivalence between the Turing computable functions and the general recursive functions was originally proved via the λ -calculus: the general recursive functions are exactly the λ -definable functions as are the Turing computable functions.

The equivalence between the λ -definable functions and the recursive functions was one of the arguments used by Church to defend his thesis proposing the identification of the intuitive class of effectively computable functions with the class of recursive functions; in fact one can give arguments for the so called Church’s superthesis which states that for the functions involved this identification preserves the intensional character, i.e. process of computation.

Historically the first undecidable problem was constructed by Church as a problem about terms of the λ -calculus (whether they have a normal form). The first definition, due to Church and Kleene, of the recursive ordinals went via the λ -calculus. The fixed point theorem of the λ -calculus inspired Kleene to the recursion theorem. Thus the λ -calculus played a central role in the early investigations of the theory of recursive functions.

Church originally designed the λ -calculus as part of a general system of functions intended to be a foundation of mathematics. The paradox of Kleene and Rosser showed that this system was inconsistent. The present theory was extracted as a consistent subtheory, CHURCH [1941]. After this,

Church seemed to have lost interest in using the λ -calculus to provide a foundation for the whole of mathematics. CURRY et al. [1958, 1972], on the other hand, have developed various systems of illative combinatory logic intended as an ultimate foundation. These systems, however, have not been developed enough to be a satisfactory basis for mathematics. See also SCOTT [1975b] for work in this direction.

Due to the type free approach it was not clear how to construct models of the theory. One would want a set X in which its function space $X \rightarrow X$ can be embedded, contradicting Cantors theorem. This difficulty was overcome by Scott in his D_∞ model constructions (in 1969), by restricting $X \rightarrow X$ to the *continuous* functions on X (provided with a proper topology). Also in the graph model $\mathcal{P}\omega$, continuity plays an essential role.

Scotts models added a new dimension to the theory, namely limit considerations. The author agrees with Scott's claim that this really makes the theory *λ -calculus* and what has been done before should be called *λ -algebra*. See Section 7 where equalities in D_∞ that cannot be proved algebraically are established by approximation methods.

Typed versions of the theory, as well as their connections with category- and proof theory are purposely not considered. The character of the typed theories is totally different from the type free version, e.g. all typed terms have a normal form. See TROELSTRA [1973] as reference for the typed theory of (primitive) recursive functionals and MANN [1975] for the relation with category- and proof theory.

It should be mentioned also that there is a theory related to the λ -calculus, in which application is only partially defined. This is the theory of uniformly reflexive structures of Wagner and Strong. This theory has an obvious model in the partial recursive indices. In fact it is intended to be an axiomatization of parts of recursion theory. See BARENDREGT [1975] for an introduction and references.

Summary

Section 1 gives an introduction to the theory and provides a general model theoretic setting. Section 2 gives a treatment of the classical λ -calculus. It will be proved that the recursive functions can be represented as λ -terms and that many sets of λ -terms are undecidable. In Section 3 the graph model $\mathcal{P}\omega$ is constructed. Section 4 treats Scott's construction of the models D_∞ as a projective limit of complete lattices. In Section 5 a λ -theory $\mathcal{H}$ is introduced. $\mathcal{H}$ has a *unique* maximal consistent extension $\mathcal{H}^*$. Section 6 associates to each term a tree, useful for the determination of its image in

the models $\mathcal{P}\omega$, D_∞ . In Section 7 it is proved that $D_\infty \models M = N$ iff $M = N \in \mathcal{H}^*$ iff M, N have equivalent trees.

1. Towards the theory

The λ -calculus studies functions and their applicative behavior, and not, as in category theory, just their behavior under composition. Therefore application is the primitive operation of the λ -calculus. The function f applied to the argument a is denoted by fa .

Schönfinkel observed that it is not necessary to introduce functions of more variables. Indeed, for a function of say two variables $f(x, y)$, one can consider g_x with $g_x(y) = f(x, y)$, and then f' with $f'x = g_x$; hence $(f'x)y = f(x, y)$. Therefore a convenient notation is $hx_1 \cdots x_n = (\cdots (hx_1) \cdots x_n)$ (association to the left), the above example becoming $f'xy = f(x, y)$. A similar construction occurs in the s-m-n theorem in recursion theory.

1.1. DEFINITION. An *applicative system* is a structure $\mathfrak{M} = \langle X, \cdot \rangle$, where $\cdot$ is a binary operation (application) on X .

The set of *terms* (using variables $a_0, a_1, \dots$) over $\mathfrak{M}$, $T(\mathfrak{M})$, is inductively defined as follows: $x_i \in T(\mathfrak{M})$; $a \in X \Rightarrow c_a \in T(\mathfrak{M})$; $A, B \in T(\mathfrak{M}) \Rightarrow (AB) \in T(\mathfrak{M})$. c_a is the constant corresponding to a . Juxtaposition of terms denotes application.

$A_1A_2 \cdots A_n$ denotes $(\cdots (A_1A_2) \cdots A_n)$ (association to the left).

1.2. DEFINITION. A *combinatory algebra* is an applicative system $\mathfrak{M}$ such that $\mathfrak{M}$ is not trivial (i.e. $\text{Card}(X) > 1$) and for each term A over $\mathfrak{M}$, with variables among $y_1, \dots, y_n$, we have in $\mathfrak{M}$:

1.3. $\exists f \forall y_1 \cdots y_n fy_1 \cdots y_n = A$ (*combinatory completeness*).

A combinatory algebra M is *extensional* if in addition in $\mathfrak{M}$

1.4. $\forall x (fx = f'x) \rightarrow f = f'$ (*extensionality*).

Combinatory completeness expresses that all algebraic functions are representable by an element. The motivation for this axiom is that for functions studied as rules, one certainly would like them to be closed under explicit definition.

It is essential that in 1.3 A is purely algebraic and not defined using logical operations. A diagonalization would otherwise make the system

trivial. However, combinatory completeness is already quite strong, e.g. there are no finite combinatory algebras and in fact no recursive ones. In contrast with e.g. the theory of fields there are $2^{\aleph_0}$ prime combinatory algebras.

In 1.3 combinatory completeness is expressed by an existential axiom. By an extension of the type of the language this can be expressed in a universal way (cf. the elementary theory of groups where the axiom $\forall x \exists y x \cdot y = e$ can be expressed by $x \cdot x^{-1} = e$ after extending the language with $^{-1}$). In fact there are two ways to do this. The first one, employed by Church, adds to the language an abstraction operator λ : if A is a term, so is $\lambda x. A$. Combinatory completeness now follows from

$$1.5. \quad (\lambda x. A)a = A[x/a] \quad (\beta\text{-conversion}).$$

Multiple abstraction can be replaced by simple ones following Schönfinkel's idea: let $\lambda x_1 \cdots x_n. A = \lambda x_1 (\lambda x_2 \cdots (\lambda x_n. A) \cdots)$; then $(\lambda x_1 \cdots x_n. A)a_1 \cdots a_n = A[x_1 \cdots x_n/a_1 \cdots a_n]$.

The other approach, due to Curry, results from realizing that combinatory completeness follows from two of its instances.

1.6. THEOREM. *Let $\mathfrak{M} = \langle X, \cdot \rangle$ be an applicative structure such that for some $k, s \in X$ one has in $\mathfrak{M}$:*

- (i) $k \neq s$,
- (ii) $kxy = x$,
- (iii) $sxyz = xz(yz)$.

Then $\mathfrak{M}$ is a combinatory algebra.

PROOF. First let $i = skk$; then $ix = skkx = kx(kx) = x$. By induction on the complexity of a term A over $\mathfrak{M}$ one can define $\lambda^*x. A$ and show that in $\mathfrak{M}$ $(\lambda^*x. A)a = A[x/a]$. Let $I \equiv c_i$, $K \equiv c_k$ and $S \equiv c_s$;

$$\lambda^*x. x = I; \quad \lambda^*x. y = Ky \quad \text{if } x, y \text{ are different variables};$$

$$\lambda^*x. c_b = Kc_b; \quad \lambda^*x. A_1A_2 = S(\lambda^*x. A_1)(\lambda^*x. A_2).$$

Therefore for the terms over $\mathfrak{M}$ one can define λ -abstraction satisfying β -conversion, hence $\mathfrak{M}$ is a λ -algebra. $\square$

Curry's theory is elegant because of its simplicity. In fact the theory of combinators with constants k and s satisfying (i)–(iii) of 1.6 is the simplest theory which is essentially undecidable. Church's notation is more intuitive however and will be used in this chapter.

The (*formal*) λ -calculus is essentially the theory which has application and abstraction as primitives and β -conversion as axiom. In addition it has the notion of *reduction* which formalizes the fact that e.g. an expression like $(\lambda x. x^2 + 1)3$ can be computed to yield 10, but not conversely. Due to the Church–Rosser theorem, reduction is very useful for the proof theory of the λ -calculus.

It should be stressed that in a theory about functions as rules, *terms* play a central role. This view differs with that of Scott, who puts the models central. It is true indeed that models are of interest not only for the insight they give on the equality of terms, but also for their mathematical structure. But the theory of D_∞ is especially beautiful because of the limit characterization of equality of *terms*; see Section 7.

Typical questions asked about terms are:

- (i) What kind of functions on terms are representable?
- (ii) Which terms are equal, which ones essentially different? Which terms can/should be equated?

Restricted to numerals, the classical answer to (i) is: the recursive functions. Question (ii) can be approached by either giving consistency proofs for reasonable extensions of the λ -calculus or by constructing models and considering the set of equations true in them. $\mathcal{H}$ and $\mathcal{H}^*$ of Section 5 were found by the first and second method respectively. Also the questions under (ii) explain why extensionality is sometimes added to the λ -calculus. Cf. the theorem of Böhm in 2.23, which states that the extensional theory is complete with respect to terms having a nf.

The theory

1.7. DEFINITION. The λ -calculus has the following language.

Alphabet:

$a_0, a_1, \dots$ variables

$\rightarrow, =$ reduction, equality;

$\lambda,), ($ auxiliary symbols.

Terms are inductively defined:

- (i) Any variable is a term;
- (ii) if M, N are terms, so is (MN) ;
- (iii) if M is a term and x a variable, then $(\lambda x M)$ is a term.

Formulas:

If M, N are terms, then $M \rightarrow N$ and $M = N$ are formulas.

1.8. CONVENTIONS. A term of the λ -calculus is called a λ -*term*. $M, N, \dots$ is a syntactic notation for arbitrary λ -terms. $x, y, z \dots$ is a syntactic notation

for arbitrary variables. $M_1 M_2 \cdots M_n$ stands for $(\cdots (M_1 M_2) \cdots M_n)$ (association to the left). $\lambda x_1 \cdots x_n . M$ stands for $(\lambda x_1 (\lambda x_2 \cdots (\lambda x_n M) \cdots))$. The symbol $\equiv$ denotes syntactic equality.

A variable occurs *free* in a term M if x is not in the scope of a λx , otherwise x occurs *bound*. In this respect λx has the same binding properties as $\forall x$ in predicate logic or $\int_a^b \cdots dx$ in calculus. We identify terms differing only in the names of their bound variables, e.g. $\lambda x . x \equiv \lambda y . y$. $FV(M)$ is the set of free variables in M , M is *closed* if $FV(M) = \emptyset$.

$M[x/N]$ denotes the result of substituting N for the *free* occurrences of x in M . In order to prevent confusion of variables we have to assume, as is the case in predicate logic, that no free variable of N becomes bound in $M[x/N]$. This can be accomplished by renaming some of the bound variables in M , e.g. $(\lambda a . ax)[x/a] \equiv \lambda a' . a'a \neq \lambda a . aa$. After this precaution, the definition of substitution is independent of the choice of representative in the equivalence class of identified terms. See also DE BRUIN [1972].

1.9. DEFINITION. The λ -calculus is defined by the following axiom schemes and rules.

- I. 1. $(\lambda x . M)N \rightarrow M[x/N]$ (β -reduction),
2. $M \rightarrow M$,
3. $M \rightarrow N, N \rightarrow L \Rightarrow M \rightarrow L$,
4. (a) $M \rightarrow M' \Rightarrow ZM \rightarrow ZM'$,
- (b) $M \rightarrow M' \Rightarrow MZ \rightarrow M'Z$,
- (c) $M \rightarrow M' \Rightarrow \lambda x . M \rightarrow \lambda x . M'$.
- II. 1. $M \rightarrow M' \Rightarrow M = M'$,
2. $M = M' \Rightarrow M' = M$,
3. $M = N, N = L \Rightarrow M = L$,
4. (a) $M = M' \Rightarrow ZM = ZM'$,
- (b) $M = M' \Rightarrow MZ = M'Z$,
- (c) $M = M' \Rightarrow \lambda x . M = \lambda x . M'$.

If $M = N$ or $M \rightarrow N$ is derivable one writes $\lambda \vdash M = N$ or $(\lambda \vdash) M \rightarrow N$ respectively. Since $=$ is generated by $\rightarrow$, the rules II.4 follow from I.4. The addition of II.4 is necessary however, if one considers extensions of the λ -calculus.

1.10. Extensionality

The λ -calculus can be extended by the following rule of extensionality,

ext: $Mx = M'x \Rightarrow M = M'$, provided $x \notin FV(M), FV(M')$

The rule ext can be axiomatized by adding the rule

$$\lambda x.Mx \rightarrow M \quad (\eta\text{-reduction})$$

provided $x \notin \text{FV}(M)$:

If $Mx = M'x$, and $x \notin \text{FV}(MM')$, then $\lambda x.Mx = \lambda x.M'x$, hence $M = \lambda x.Mx = \lambda x.M'x = M'$.

The λ -calculus with this additional reduction rule is called the $\lambda\eta$ -calculus. Provability in this theory is denoted by $\lambda\eta \vdash \dots$.

M and N are $\beta(\eta)$ -convertible iff $\lambda(\eta) \vdash M = N$.

The models

Our main object of study is the λ -calculus. Therefore we would want that the combinatory algebras are also models for this theory, i.e. that there is an interpretation of the λ -operator. However unless a combinatory algebra is extensional, there is a choice for the element f representing the function A in 1.3. Thus the combinatory algebras have not enough structure to be models for the λ -calculus.

1.11. DEFINITION. A *pre- λ -algebra* is a combinatory algebra $\mathfrak{M}$ together with a method of assigning to each term $A \in T(\mathfrak{M})$ a term $\lambda * x.A \in T(\mathfrak{M})$ such that

- (i) x does not occur in $\lambda * x.A$,
- (ii) $\mathfrak{M} \models (\lambda * x.A)x = A$.

Remarks. (1) For most $\mathfrak{M}$ this assignment $A \mapsto \lambda * x.A$ is provided for by the *proof* that $\mathfrak{M}$ is a combinatory algebra.

(2) Although the definition of a pre- λ -algebra is not formulated in a conventional first order way, from a constructive point of view it is completely clear.

1.12. DEFINITION. *Interpretation of λ -terms.* Let ρ be a valuation of the variables into a pre- λ -algebra $\mathfrak{M} = \langle X, \cdot \rangle$ i.e. $\rho = \{a_0, a_1, \dots\} \rightarrow X$. The value in $\mathfrak{M}$ of a λ -term M under the valuation ρ , notation $\llbracket M \rrbracket_\rho^{\mathfrak{M}}$, is defined in two steps. First M is transformed into a term $\langle\langle M \rangle\rangle^{\mathfrak{M}} \in T(\mathfrak{M})$. Then this term is interpreted in M under the valuation ρ in the usual first order way, yielding $\llbracket M \rrbracket_\rho^{\mathfrak{M}}$.

$\langle\langle M \rangle\rangle^{\mathfrak{M}}$ is inductively defined as follows: $\langle\langle x \rangle\rangle^{\mathfrak{M}} = x$; $\langle\langle MN \rangle\rangle^{\mathfrak{M}} = \langle\langle M \rangle\rangle^{\mathfrak{M}} \langle\langle N \rangle\rangle^{\mathfrak{M}}$; $\langle\langle \lambda x.M \rangle\rangle^{\mathfrak{M}} = \lambda * x. \langle\langle M \rangle\rangle^{\mathfrak{M}}$.

1.13. DEFINITION. Satisfaction. As usual, $\mathfrak{M} \models M = N$ iff for all ρ , $\llbracket M \rrbracket_\rho^{\mathfrak{M}} = \llbracket N \rrbracket_\rho^{\mathfrak{M}}$.

1.14. DEFINITION. A λ -algebra or *model of the λ -calculus* is a pre- λ -algebra $\mathfrak{M}$ such that $\lambda \vdash M = N \Rightarrow \mathfrak{M} \models M = N$.

Remark. The term model $\mathfrak{M}(\text{CL})$ of the theory of combinators is a pre- λ -algebra (by the proof of 1.6) but not a λ -algebra, since $\mathfrak{M}(\text{CL}) \not\models \lambda x. ((\lambda y. y)x) = \lambda x. x : s(ki)i \neq i$.

1.15. DEFINITION. (i) A *weakly extensional* (w.e.) λ -algebra is a λ -algebra $\mathfrak{M}$ such that

$$\mathfrak{M} \models M = M' \Rightarrow \mathfrak{M} \models \lambda x. M = \lambda x. M'.$$

(ii) A λ -algebra $\mathfrak{M}$ is *extensional* iff $\mathfrak{M}$ satisfies $\forall x (fx = gx) \rightarrow f = g$ (extensionality).

1.16. REMARK. (1) An extensional λ -algebra is clearly w.e.

(2) A combinatory algebra satisfying extensionality is an extensional λ -algebra, since there is only one way to define abstraction.

(3) There are interesting λ -algebras that are not weakly extensional, e.g. $\mathfrak{M}^0(\lambda)$ (see below) as follows by the ω -incompleteness of the λ -calculus (cf. PLOTKIN [1974]) or $\mathcal{P}_\omega^0$.

(4) The only λ -algebras that are considered here are either w.e. or term models.

1.17. General concepts and notations

ω denotes the set of natural numbers. $\lambda x. \dots$ denotes the mapping $x \mapsto \dots$ (meta lambda).

Notions connected with theories

Λ is the set of λ -terms. Λ^0 is the set of closed λ -terms. Let $\mathbf{T}$ be a set of equations between λ -terms. Then $\lambda + \mathbf{T}$ is the λ -calculus extended with the equations in $\mathbf{T}$ as axioms. $\mathbf{T}^+ = \{M = N \mid M, N \in \Lambda^0 \text{ and } \lambda + \mathbf{T} \vdash M =$

$N\}$. $\mathbf{T}$ is said to be *consistent* if $\mathbf{T}^+$ does not contain every equation. A λ -*theory* is a consistent set of equations $\mathbf{T}$ such that $\mathbf{T} = \mathbf{T}^+$.

λ is the λ -theory $\{M = N \mid M, N \in \Lambda^0 \text{ and } \lambda \vdash M = N\}$; the consistency is shown in 2.9.

For a λ -theory $\mathbf{T}$ define $M \sim_{\mathbf{T}} N$ iff $\lambda + \mathbf{T} \vdash M = N$. $\sim_{\mathbf{T}}$ is an equivalence relation and let $[M]^{-\mathbf{T}}$ denote the equivalence class of M with respect to $\sim_{\mathbf{T}}$. The *term model* of $\mathbf{T}$, $\mathfrak{M}(\mathbf{T})$, is the λ -algebra consisting of all λ -terms modulo $\sim_{\mathbf{T}}$, with application and abstraction defined canonically. The *closed term model* of $\mathbf{T}$, $\mathfrak{M}^0(\mathbf{T})$, is the set of terms without free variables modulo $\sim_{\mathbf{T}}$.

A λ -theory $\mathbf{T}$ is *maximally consistent* if $\mathbf{T}$ has no proper consistent extensions.

Notions connected with models

For a λ -algebra $\mathfrak{M}$, $\text{Th}(\mathfrak{M})$ is the λ -theory $\{M = N \mid M, N \in \Lambda^0 \text{ and } \mathfrak{M} \models M = N\}$. The consistency follows from the fact that $\text{Card}(\mathfrak{M}) > 1$ (see 2.3).

The *interior* of $\mathfrak{M}$, notation $\mathfrak{M}^0$, is the substructure consisting of the images in $\mathfrak{M}$ of the closed λ -terms. Up to isomorphism $\mathfrak{M}^0 = \mathfrak{M}^0(\text{Th}(\mathfrak{M}))$. $\mathfrak{M}$ is *hard* iff $\mathfrak{M} = \mathfrak{M}^0$. The hard λ -algebras are the prime structures among the λ -algebras.

For λ -algebras a homomorphism $h : \mathfrak{M} \rightarrow \mathfrak{M}'$ should not only preserve application, but also abstraction, i.e. for a term $A \in T(\mathfrak{M})$, $h(\lambda^*x.A) = \lambda^*x.hA$ in $\mathfrak{M}'$ where for $B \in T(\mathfrak{M})$, $hB \in T(\mathfrak{M}')$ is the term obtained by replacing in B all constants c_a by c_{ha} .

We will use homomorphisms only in connection with term models. There the description is simple. If $\mathbf{S} \subset \mathbf{T}$ are λ -theories, then a $h : \mathfrak{M}(\mathbf{S}) \rightarrow \mathfrak{M}(\mathbf{T})$ is defined by $h([M]^{-\mathbf{S}}) = [M]^{-\mathbf{T}}$. Thus each (closed) term model $\mathfrak{M}^{(0)}(\mathbf{S})$ is the homomorphic image of $\mathfrak{M}^{(0)}(\lambda) : [M]^{-\lambda} \rightarrow [M]^{-\mathbf{S}}$. If $\mathbf{S}$ is maximally consistent, then $\mathfrak{M}^{(0)}(\mathbf{S})$ is algebraically *simple*, i.e. has no proper homomorphic images.

2. Classical λ -calculus

The classical theory is mainly concerned with $\mathfrak{M}(\lambda)$. Among others the following theorems will be proved. All recursive functions are λ -definable (Kleene). The set of terms with(out) a normal form is undecidable (Church). There is no recursive model for the λ -calculus (Grzegorzcyk). The last two theorems follows most easily from a theorem of Scott. Finally

the theorem of Böhm is stated, which shows the completeness of $\beta\eta$ -conversion for terms having a normal form.

2.1. FIXED POINT THEOREM. *For every $F \in \Lambda$ there is an $M \in \Lambda$ such that $\lambda \vdash FM = M$.*

PROOF. Define $\omega = \lambda x. F(xx)$ and $M = \omega\omega$. Then $\lambda \vdash M = \omega\omega = (\lambda x. F(xx))\omega = F(\omega\omega) = FM$. $\square$

Remarks. (1) The fixed points can be found in a uniform way: let $Y = \lambda f. (\lambda x. f(xx))(\lambda x. f(xx))$; then $\lambda \vdash Yf = f(Yf)$.

(2) Since the theorem holds for terms possibly containing free variables, each element of a λ -algebra has a fixed point.

(3) Curry calls Y the *paradoxical combinator*.

Note that in 2.1, $\lambda \vdash M \rightarrow FM$. This explains why the related constructions in the recursion theorem or Gödel's self-referential sentence are somewhat puzzling, cf. BARENDREGT [to appear], §6.7.

2.2. Frequently we need some standard terms. Let $I = \lambda x. x$, $K = \lambda xy. x$, $S = \lambda xyz. xz(yz)$ and $\Omega = (\lambda x. xx)(\lambda x. xx)$. Then $\lambda \vdash IM = M$, $\lambda \vdash KMM = M$ and $\lambda \vdash SMNL = ML(NL)$.

From 1.6 it follows that each closed term can be defined in terms of I , K and S .

2.3. Truth values **t** (true) and **f** (false). Define **t** = K , **f** = KI . Then $\lambda \vdash \mathbf{t}MN = M$ and $\lambda \vdash \mathbf{f}MN = N$. Note that **t** $\neq$ **f** in any λ -algebra $\mathfrak{M}$, for otherwise $\mathfrak{M}$ would satisfy $x = \mathbf{t}xy = \mathbf{f}xy = y$ and hence be trivial.

2.4. Conditional

If B is a term taking values **t** and **f**, then the intuitive value of “If B then M else N ” can be represented by BMN .

2.5. Ordered pairs

Define $[M, N] = \lambda x. xMN$, $(M)_0 = M\mathbf{t}$ and $(M)_1 = M\mathbf{f}$. Then $\lambda \vdash ([M_0, M_1])_i = M_i$, $i = 0, 1$.

2.6. Numerals

Define $\underline{0} = I$ and $\underline{n+1} = [\underline{n}, K]$. The numerals are chosen this way to

provide a convenient base for the representation of the recursive functions. CHURCH [1941] used the following numerals: $\underline{n} = \lambda fx. f^n x$, where $f^0 x = x$ and $f^{n+1} x = f(f^n x)$.

2.7. DEFINITION. (i) A *redex* is a term of the form $(\lambda x. P)Q$ (in the extensional theory also $(\lambda x. Px)$, with $x \notin \text{FV}(P)$, is a redex).

(ii) A term M is *in normal form* (nf) iff there is no subterm of M which is a redex (if it is necessary to distinguish nf's in the λ - and $\lambda\eta$ -calculus one talks about β - and $\beta\eta$ -nf's).

(iii) A term M *has a* nf iff for some N in nf $\lambda \vdash M \rightarrow N$ (in the extensional theory $\lambda\eta \vdash M \rightarrow N$).

Intuitively a term is in nf if it cannot be computed any further.

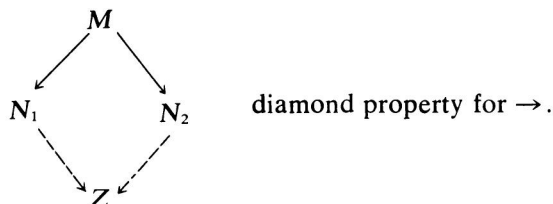
Example. $(\lambda x. xx)y$ has the nf yy ; Ω has no nf. Note that for every natural number n , $\underline{n}$ is in nf.

Now an important theorem on reduction will be stated. For details see e.g. HINDLEY et al. [1972] p. 139 or BARENDREGT [to appear].

2.8. CHURCH-ROSSER THEOREM. *If $\lambda \vdash M = N$, then for some Z , $\lambda \vdash M \rightarrow Z$ and $\lambda \vdash N \rightarrow Z$ (and similarly for the $\lambda\eta$ -calculus).*

PROOF (outline; after Tait and Martin-Löf). The theorem follows from (and in fact is equivalent with):

(*) If $M \rightarrow N_1$, $M \rightarrow N_2$, then for some Z , $N_1 \rightarrow Z$ and $N_2 \rightarrow Z$:



That 2.8 follows from (*) is proved by induction on the length of proof of $\lambda \vdash M = N$, (*) being needed for the transitivity of $=$.

(*) is proved by defining a relation $\rightarrow$ on λ -terms, such that (i) $\rightarrow$ has the diamond property; (ii) $\rightarrow$ is the transitive closure of $\rightarrow$. The diamond property for $\rightarrow$ then follows by a simple diagram chasing.

The relation $\rightarrow$ is defined inductively as follows:

$$M \rightarrow M: \quad M \rightarrow M', N \rightarrow N' \Rightarrow (\lambda x. M)N \rightarrow M'[x/N'];$$

$$M \rightarrow M', N \rightarrow N' \Rightarrow MN \rightarrow M'N': \quad M \rightarrow M' \Rightarrow \lambda x. M \rightarrow \lambda x. M'.$$

Then (ii) is obvious and (i) follows from a case analysis and $M \rightarrow M'$, $N \rightarrow N' \Rightarrow M[x/N] \rightarrow M'[x/N']$, as can be proved by induction on the generation of $\rightarrow$. $\square$

2.9. COROLLARY. (i) *If M has a nf at all, then M has a unique nf.*

(ii) *If $\lambda \vdash M = N$ and N is in nf, then $M \rightarrow N$.*

(iii) *The λ -calculus is consistent, i.e. $\lambda \not\vdash M = N$ for some equation.*

PROOF. (i) Note that if N is a nf and $N \rightarrow N'$, then $N' \equiv N$. Now suppose $M \rightarrow N_1$, $M \rightarrow N_2$ and N_1, N_2 are nf, then $\lambda \vdash N_1 = N_2$, so by 2.8, $N_1 \rightarrow Z$ and $N_2 \rightarrow Z$. But then $N_1 \equiv Z \equiv N_2$.

(ii) If $M = N$, again $M \rightarrow Z$ and $N \rightarrow Z$. But since N is a nf, $N \equiv Z$, so $M \rightarrow N$.

(iii) If M, N are distinct nf's, then $\lambda \not\vdash M = N$ by (ii) and (i). $\square$

2.10. DEFINITION. Let ω be the set of natural numbers. A function $f: \omega^n \rightarrow \omega$ is λ -definable iff for some $F \in \Lambda^0$,

$$(*) \quad \lambda \vdash F\bar{k}_1 \cdots \bar{k}_n = \bar{m} \Leftrightarrow f(k_1, \dots, k_n) = m.$$

If $(*)$ holds, then f is said to be λ -definable by F .

2.11. REMARK. If for some λ -term F instead of $(*)$ we have

$$(**) \quad f(k_1, \dots, k_n) = m \Rightarrow \lambda \vdash F\bar{k}_1 \cdots \bar{k}_n = \bar{m},$$

then f is λ -definable by F : suppose $\lambda \vdash F\bar{k}_1 \cdots \bar{k}_n = \bar{m}$ and $f(k_1, \dots, k_n) = m'$. Then by $(**)$, $\lambda \vdash F\bar{k}_1 \cdots \bar{k}_n = \bar{m}'$ and hence by 2.9(i) $m = m'$, since the numerals are in normal form. So $f(k_1, \dots, k_n) = m$.

2.12. LEMMA. *The initial functions $U_i^n(x_1, \dots, x_n) = x_i$, $Z(x) = 0$, $S^+(x) = x + 1$ are λ -definable.*

PROOF. Take as defining terms $U_i^n = \lambda x_1 \cdots x_n. x_i$, $Z = \lambda x. 0$ and $S^+ = \lambda x. [x, K]$ respectively and use 2.11. $\square$

2.13. LEMMA. *The λ -definable functions are closed under composition.*

PROOF. The representation of the composition is the composition of the representations. $\square$

2.14. LEMMA. *There are terms P and Zero , such that $P(S^+x) = x$ and $\text{Zero } x = \mathbf{t}$ if $x = \mathbf{0}$, $\text{Zero } x = \mathbf{f}$ if x is a numeral $\neq \mathbf{0}$.*

PROOF. Take $P = \lambda x. (x)_0$, $\text{Zero} = \lambda x. (x)_1 \mathbf{f} \mathbf{t}$. $\square$

2.15. LEMMA. *The λ -definable functions are closed under primitive recursion.*

PROOF. For simplicity we omit parameters. Let f be defined by $f(0) = k$, $f(n+1) = g(f(n), n)$, where g is λ -definable by G . We want to define F such that it satisfies $Fx = \text{if Zero } x, \text{ then } k, \text{ else } G(F(Px))(Px)$. By 2.4 this can be expressed as $Fx = \text{Zero } x \ k [G(F(Px))(Px)]$ or $F = \lambda x. \text{Zero } x \ k [G(F(Px))(Px)]$. Define $\Theta = \lambda f x. \text{Zero } x \ k [G(f(Px))(Px)]$. Then we can take F as being the fixed point of Θ . $\square$

2.16. LEMMA. *The λ -definable functions are closed under minimalization.*

PROOF. (Again we omit parameters.) Let f be defined by $f(x) = \mu y [g(x, y) = 0]$, where g is λ -defined by G and $\forall n \exists m g(n, m) = 0$. As in 2.15 we can find a λ -term H such that $Hxy = \text{if Zero}(Gxy), \text{ then } y, \text{ else } Hx(S^+y)$. Then take $F = \lambda x. Hx \mathbf{0}$. $\square$

Remark. It is clear that the λ -calculus is a recursively axiomatizable theory. Hence (after Gödelization) the relation $\{(M, N) \mid \lambda \vdash M = N\}$ is recursively enumerable.

2.17. THEOREM (Kleene). *The λ -definable functions are exactly the recursive functions.*

PROOF. If f is recursive, then f is λ -definable, since the recursive functions are the least class containing the initial functions which is closed under composition, primitive recursion and minimalization. If f is λ -defined by F , then $f(k_1, \dots, k_n) = m \Leftrightarrow \lambda \vdash F \underline{k}_1 \cdots \underline{k}_n = \underline{m}$ hence by the preceding remark the graph of f is r.e., so f is recursive. $\square$

Remark. A partial function $\psi : \omega^k \rightarrow \omega$ is λ -definable iff for some term F , $\psi(\vec{k}) = m \Leftrightarrow \lambda \vdash F \vec{k} = \underline{m}$, and $\psi(\vec{k})$ undefined $\Leftrightarrow F \vec{k}$ has no nf.

It can be shown that for partial functions, ψ is λ -definable iff ψ is partial recursive. In order to do this one must show that certain terms have no nf. For this purpose the following reduction strategy is useful.

2.18. DEFINITION. Let M be a λ -term. If M is not a nf, let M' be obtained by reducing the leftmost redex in M (i.e. the redex with its λ as left as possible), else M' is undefined. Define $M_0 = M$, $M_{n+1} = (M_n)'$. The sequence $M_0 \rightarrow M_1 \rightarrow \dots$ (finite or infinite) is called the *leftmost* or *normal* reduction chain of M .

2.19. NORMALIZATION THEOREM (Curry). *M has a nf iff the leftmost reduction chain of M is finite.*

PROOF. See CURRY et al. [1958] p.142. $\square$

The theorem is false for arbitrary reduction chains, consider e.g. $KI\Omega$ having a nf but also an infinite reduction chain.

Undecidability results

After coding syntactical objects as natural numbers one can speak of the decidability of a set of terms or equations. It will be shown that the λ -calculus is essentially undecidable, i.e. has no decidable consistent extension.

It is standard to define a coding $M \rightarrow \#M$ such that there are recursive functions $\text{Ap}(\#M, \#N) = \#(MN)$ and $\text{Num}(n) = \#\underline{n}$. The numeral $\underline{\#M}$ will be denoted by $\ulcorner M \urcorner$.

2.20. SECOND FIXED POINT THEOREM. *For each $F \in \Lambda^{(0)}$ there is an $X \in \Lambda^{(0)}$ such that $\lambda \vdash F \ulcorner X \urcorner = X$.*

PROOF. Let the recursive functions Ap and Num be λ -defined by the terms Ap and Num . Define $\omega = \lambda x. F(\text{Ap}x(\text{Num}x))$ and $X = \omega \ulcorner \omega \urcorner$. Then

$$\lambda \vdash X = \omega \ulcorner \omega \urcorner \rightarrow F(\text{Ap} \ulcorner \omega \urcorner (\text{Num} \ulcorner \omega \urcorner)) \rightarrow F \ulcorner \omega \ulcorner \omega \urcorner \urcorner = F \ulcorner X \urcorner,$$

since $\text{Num} \ulcorner \omega \urcorner \rightarrow \ulcorner \omega \urcorner$. $\square$

A set $\mathcal{A} \subseteq \Lambda^0$ is *closed under equality* iff $M \in \mathcal{A}$ and $M = N \in \Lambda \Rightarrow N \in \mathcal{A}$. $\mathcal{A} \subseteq \Lambda^0$ is *non-trivial* iff $\mathcal{A} \neq \emptyset$ and $\mathcal{A} \neq \Lambda^0$.

2.21. THEOREM (Scott). *Let $\mathcal{A} \subseteq \Lambda^0$ be a non-trivial set closed under equality. Then $\mathcal{A}$ is not recursive.*

PROOF. Let $M_0 \in \mathcal{A}$, $M_1 \in \Lambda^0 - \mathcal{A}$. Suppose $\mathcal{A}$ were recursive. Then there is a recursive function $f : \omega \rightarrow \{0, 1\}$ such that $f(\#M) = 0$ iff $M \in \mathcal{A}$. Let f be λ -defined by F . Define $F' = \lambda x. \text{If Zero}(Fx), \text{ then } M_1 \text{ else, } M_0$. Then $F'(\ulcorner M \urcorner) = M_1$ if $M \in \mathcal{A}$ and $F'(\ulcorner M \urcorner) = M_0$ if $M \notin \mathcal{A}$. $\exists X \in \Lambda^0 F' \ulcorner X \urcorner = X$, by 2.20. If $X \in \mathcal{A}$, then $X = F' \ulcorner X \urcorner = M_1 \notin \mathcal{A}$ and if $X \notin \mathcal{A}$ then $X = F' \ulcorner X \urcorner = M_0 \in \mathcal{A}$, contradicting in both cases that $\mathcal{A}$ is closed under equality. $\square$

2.22. COROLLARY (Church; Grzegorzczuk). (i) *The set of terms with(out) a nf is not recursive.*

(ii) *There are no recursive λ -theories.*

(iii) *There are no recursive λ -algebras.*

PROOF. (i) $\{M \mid M \text{ has a (has no) nf}\}$ satisfies the condition of 2.21.

(ii) Let $\mathbf{T}$ be a λ -theory. Then $\{M \mid M = I \in \mathbf{T}\}$ satisfies 2.21. Hence $\mathbf{T}$ is not recursive.

(iii) If $\mathcal{M}$ were a recursive λ -algebra, then $\text{Th}(\mathcal{M})$ would be a recursive λ -theory, contradicting (ii). $\square$

The following result shows the completeness of the $\lambda\eta$ -calculus with respect to terms having a nf.

2.23. THEOREM (Böhm). *If M, N are different $\beta\eta$ -nf's, then $\lambda + M = N$ is inconsistent.*

PROOF (outline). If $M \neq N$ are $\beta\eta$ -nf's, then M, N have finite Böhm trees which are not η -equivalent, see Section 6. Hence by 6.8, $M = N \notin \mathcal{H}^*$. In fact it follows from the proof of 6.8 that in this case $\lambda \vdash C[M] = x$ and $\lambda \vdash C[N] = y$ for some context $C[\cdot]$ and variables $x \neq y$. So $\lambda + M = N \vdash x = y$, i.e. $\lambda + M = N$ is inconsistent. $\square$

For terms without nf this completeness result is false, see 7.2.

3. Construction of the graph model $\mathcal{P}\omega$

The first λ -algebras were the lattice models D_∞ constructed by Scott in 1969, see Section 4. The graph model $\mathcal{P}\omega$ is less involved and therefore will be described first. This model was found by PLOTKIN [1972] and, in a more

explicit form, by Scott. For connections of this model with recursion theoretic ideas, see SCOTT [1975a], [1976].

The role of continuity in the model construction was already mentioned in Section 1. The topology on $\mathcal{P}\omega$ is such that a continuous function $\mathcal{P}\omega \rightarrow \mathcal{P}\omega$ can be coded as an element of $\mathcal{P}\omega$. This is the essential feature of the model.

3.1. DEFINITION. (i) $\mathcal{P}\omega = \{x \mid x \subseteq \omega\}$.

(ii) There are countably many finite elements of $\mathcal{P}\omega$. As an effective one-one enumeration of these sets we use e_n , where

$$e_n = \{k_0, \dots, k_{m-1}\} \quad \text{with } k_0 < \dots < k_{m-1} \Leftrightarrow n = \sum_{i < m} 2^{k_i}.$$

(iii) $(\cdot, \cdot)$ is the coding of pairs of integers into the integers defined by $(n, m) = \frac{1}{2}(n+m)(n+m+1) + m$.

3.2. DEFINITION. Let $e \subseteq \omega$ be a finite subset.

$$O_e = \{x \in \mathcal{P}\omega \mid e \subseteq x\}; \quad O_n = O_{e_n}.$$

3.3. LEMMA. *The $\{O_n\}_{n \in \omega}$ form a base for a topology on $\mathcal{P}\omega$.*

PROOF. $O_e \cap O_{e'} = O_{e \cup e'}$. $\square$

Henceforth we always will consider $\mathcal{P}\omega$ provided with this topology.

3.4. LEMMA. $f: \mathcal{P}\omega \rightarrow \mathcal{P}\omega$ is continuous $\Leftrightarrow f(x) = \bigcup \{f(e_n) \mid e_n \subseteq x\}$.

PROOF. ($\Rightarrow$) First note that f is monotonic. For suppose $x \subseteq y$ and $n \in f(x)$. Then $f(x) \in O_{(n)}$. By continuity for some e , $x \in O_e$ and $f(O_e) \subseteq O_{(n)}$. Now $e \subseteq x \subseteq y$, so $y \in O_e$, hence $f(y) \subseteq O_{(n)}$, i.e. $n \in f(y)$. Therefore indeed $x \subseteq y \Rightarrow f(x) \subseteq f(y)$.

By monotonicity of f , $f(x) \supseteq \bigcup \{f(e_n) \mid e_n \subseteq x\}$. To show the reverse, suppose $n \in f(x)$. Again for some e , $x \in O_e$ and $f(O_e) \subseteq O_{(n)}$. Hence since $e \subseteq O_e$, we have $f(e) \in O_{(n)}$, i.e. $n \in f(e) \subseteq \bigcup \{f(e_n) \mid e_n \subseteq x\}$.

($\Leftarrow$) Again f is monotonic. For suppose $x \subseteq y$ and $n \in f(x)$. By the assumption, $n \in f(e)$ for some finite $e \subseteq x$. Hence $n \in \bigcup \{f(e') \mid e' \subseteq y\} = f(y)$.

Now suppose $f(x) \in O_e$, i.e. $e \subseteq f(x)$. Let $e = \{m_1, \dots, m_k\}$. By assumption $m_i \in f(e_{n_i})$ for some $e_{n_i} \subseteq x$. Then $f(O_{e_{n_i}}) \subseteq O_{(m_i)}$ by monotonicity.

Then $O = O_{e_{n_1}} \cap \cdots \cap O_{e_{n_k}}$ is a neighborhood of x and

$$f(O) \subseteq f(O_{e_{n_1}}) \cap \cdots \cap f(O_{e_{n_k}}) \subseteq O_{\{m_1\}} \cap \cdots \cap O_{\{m_k\}} = O_{\{m_1, \dots, m_k\}} = O_e.$$

So $\forall O_e \ni f(x) \exists x \ni O f(O) \subseteq O_e$, i.e. f is continuous. $\square$

By the previous lemma, a continuous function f is completely determined by its values on the finite sets. Hence if one knows for what $m, n \in f(e_n)$, then the $f(e_n)$ are known and therefore f . Thus the information of a continuous function can be coded into a set. This operation is called graph. Its inverse operation is fun.

3.5. DEFINITION. (i) Let $f: \mathcal{P}\omega \rightarrow \mathcal{P}\omega$ be continuous, then $\text{graph}(f) = \{(n, m) \mid m \in f(e_n)\}$.

(ii) Let $u \in \mathcal{P}\omega$. The function $\text{fun}(u)$ is defined by $\text{fun}(u)(x) = \{m \mid \exists e_n \subseteq x (n, m) \in u\}$.

3.6. THEOREM. (i) A continuous function f is uniquely determined by its graph: $\text{fun}(\text{graph}(f)) = f$.

(ii) For every $u \in \mathcal{P}\omega$, $\text{fun}(u)$ is continuous.

PROOF. (i)

$$\begin{aligned} \text{fun}(\text{graph}(f))(x) &= \{m \mid \exists e_n \subseteq x (n, m) \in \text{graph}(f)\} \\ &= \{m \mid \exists e_n \subseteq x m \in f(e_n)\} \\ &= \{f(e_n) \mid e_n \subseteq x\} = f(x), \quad \text{by 3.4.} \end{aligned}$$

(ii) Let $f = \text{fun}(u)$. Then $f(x) = \bigcup \{u_n \mid e_n \subseteq x\}$, where $u_n = \{m \mid (n, m) \in u\}$. Now

$$\begin{aligned} m \in f(x) &\Leftrightarrow \exists n [e_n \subseteq x \wedge m \in u_n] \Leftrightarrow \exists n [(e_n \subseteq e_n \wedge m \in u_n) \wedge e_n \subseteq x] \\ &\Leftrightarrow \exists n [e_n \subseteq x \wedge m \in f(e_n)] \Leftrightarrow m \in \bigcup \{f(e_n) \mid e_n \subseteq x\}. \end{aligned}$$

So $f(x) = \bigcup \{f(e_n) \mid e_n \subseteq x\}$ and 3.4 applies. $\square$

In general $\text{graph}(\text{fun}(u)) = u$ does not hold, only $\supseteq$.

3.7. DEFINITION. Application in $\mathcal{P}\omega$ is defined by $u \cdot x = \text{fun}(u)(x)$.

3.8. LEMMA. A function $f: \mathcal{P}\omega^k \rightarrow \mathcal{P}\omega$ is continuous iff f is continuous in each of its variables separately (i.e. $\lambda x. f(x, y_0)$ and $\lambda y. f(x_0, y)$ are continuous for all x_0, y_0).

PROOF. ($\Rightarrow$) As ever.

($\Leftarrow$) It is sufficient to prove this for $k = 2$. Let $f(x, y)$ be continuous in x and y separately. Then

$$f(x, y) = \bigcup \{f(e_n, y) \mid e_n \subseteq x\} = \bigcup \{f(e_n, e_m) \mid e_n \subseteq x, e_m \subseteq y\}.$$

As in the proof of 3.4 $\Leftarrow$, it now follows that f is continuous in the product topology sense. $\square$

3.9. LEMMA (Continuity of application). *Define $\text{Ap}: \mathcal{P}\omega^2 \rightarrow \mathcal{P}\omega$ by $\text{Ap}(u, x) = u \cdot x$; then Ap is continuous.*

PROOF. $\lambda x. \text{Ap}(u, x) = \lambda x(u \cdot x) = \text{fun}(u)$ which is continuous by 3.6(ii).

$$\lambda u. \text{Ap}(u, x) = \lambda u. (u \cdot x) = \lambda u \{m \mid \exists e_n \subseteq x (n, m) \in u\}$$

which is clearly continuous. Now the result follows from 3.8. $\square$

3.10. LEMMA (Continuity of abstraction). *Let $f(x, \vec{y}): \mathcal{P}\omega^{k+1} \rightarrow \mathcal{P}\omega$ be continuous. Define $g(\vec{y}) = \text{graph}(\lambda x. f(x, \vec{y}))$. Then $g: \mathcal{P}\omega^k \rightarrow \mathcal{P}\omega$ is continuous.*

PROOF. For simplicity we set $k = 1$. Note that by 3.8, g is well defined. Now

$$\begin{aligned} g(y) &= \text{graph}(\lambda x. f(x, y)) = \{(n, m) \mid m \in f(e_n, y)\} \\ &= \{(n, m) \mid m \in \bigcup \{f(e_n, e) \mid e \subseteq y\}\} = \{(n, m) \mid \exists e \subseteq y m \in f(e_n, e)\} \\ &= \bigcup \{\{(n, m) \mid m \in f(e_n, e)\} \mid e \subseteq y\} = \bigcup \{g(e) \mid e \subseteq y\}. \end{aligned}$$

Hence 3.4 applies. $\square$

3.11. THEOREM. $\langle \mathcal{P}\omega, \cdot \rangle$ is a w.e. λ -algebra.

PROOF. For a continuous $f: \mathcal{P}\omega^{k+1} \rightarrow \mathcal{P}\omega$, define $\lambda^* d. f(d, \vec{e}) = \text{graph}(\lambda d. f(d, \vec{e}))$. By 3.10 this is a continuous function in $\vec{e}$ and by 3.7 and 3.6(i) one has $(\lambda^* d. f(d, \vec{e})).d = f(d, \vec{e})$. Now for $A \equiv A(x, y_1, \dots, y_k) \in T(\mathcal{P}\omega)$, where $\{\vec{y}\} = \text{FV}(A) - \{x\}$, define $\lambda^* x. A = c_a \cdot \vec{y}$, where $a = \lambda^* e_1 \cdots \lambda^* e_k \lambda^* d. (A(c_d, c_{e_1}, \dots, c_{e_k})^{\mathcal{P}\omega})$ and $\cdots^{\mathcal{P}\omega}$ denotes the

interpretation in $\mathcal{P}\omega$. This makes $\mathcal{P}\omega$ into a λ -algebra. Since λ^* is defined by functions in extension, $\mathcal{P}\omega$ with λ^* is w.e. $\square$

SCOTT [1975a] considers an extension of the lambda calculus, called LAMBDA, together with an interpretation in $\mathcal{P}\omega$. It is proved that the interior of $\mathcal{P}\omega$ with respect to LAMBDA consists exactly of the recursively enumerable sets.

4. Construction of D_∞

The results in this section are due to SCOTT [1972]. Again continuity is the essential feature in the model construction.

First complete lattices and their induced topologies are considered. Then follows the construction of the λ -algebras D_∞ as a projective (and at the same time direct) limit of these lattices.

4.1. DEFINITION. Let D be a complete lattice, i.e. a partially ordered set $\langle D, \sqsubseteq \rangle$ such that each subset $X \subset D$ has a supremum $\bigsqcup X \in D$. Then each subset X has an infimum as well:

$$\bigsqcup X = \bigsqcup \{z \mid z \sqsubseteq X\} \quad \text{where } z \sqsubseteq X \Leftrightarrow \forall x \in X z \sqsubseteq x.$$

Top, $\top = \bigsqcup D$, and bottom $\perp = \bigsqcap D$ are resp. the largest and smallest elements of D . A subset $X \subset D$ is *directed* iff $\forall x, y \in X \exists z \in X x, y \sqsubseteq z$. Further, $x \sqcup y$ ($x \sqcap y$) is the supremum (infimum) of $\{x, y\}$. $D, D', D'', \dots$ will range over complete lattices.

4.2. DEFINITION. A subset $U \subset D$ is *open* iff

- (i) $x \in U$ and $x \sqsubseteq y \Rightarrow y \in U$, and
- (ii) $\bigsqcup X \in U \Rightarrow X \cap U \neq \emptyset$ for all directed $X \subset D$.

D and $\emptyset$ are open, and open sets are closed under arbitrary unions; if U_1, U_2 are open, then $U_1 \cap U_2$ is open by the fact that in (ii), X is directed. Hence the partial ordering induces a topology on D . Note that the sets $U_x = \{z \mid z \not\sqsubseteq x\}$ are open and $x \notin U_x$. Therefore the topology is T_0 : if x, y are different, say $x \not\sqsubseteq y$, then $x \in U_y, y \notin U_y$. The space is not T_1 : if $x \sqsubseteq y$ and $x \in U$, open, then $y \in U$.

4.3. LEMMA. A mapping $f: D \rightarrow D'$ is continuous $\Leftrightarrow f(\bigsqcup X) = \bigsqcup f(X)$

for all directed $X \subset D$ (where $f(X) = \{f(x) \mid x \in X\}$ and the second $\sqcup$ is to be taken in D').

PROOF. ($\Rightarrow$) Let f be continuous. Suppose $x \sqsubseteq y$ in order to show $f(x) \sqsubseteq f(y)$. If not, then $f(x) \in U_{f(y)}$, so $x \in f^{-1}(U_{f(y)})$ which is open. Therefore $y \in f^{-1}(U_{f(y)})$, i.e. $f(y) \in U_{f(y)}$, a contradiction. Hence f is monotonic. It follows that, since $\sqcup X \supseteq X$, $f(\sqcup X) \supseteq f(X)$. Therefore $f(\sqcup X) \supseteq \sqcup f(X)$. If $f(\sqcup X) \not\supseteq \sqcup f(X)$, then $f(\sqcup X) \in U_{\sqcup f(X)}$ and a contradiction can be obtained as above, using condition (ii) for open sets.

($\Leftarrow$) Again f is monotonic, since if $x \sqsubseteq y$, then $y = x \sqcup y$, hence $f(y) = f(x) \sqcup f(y)$, so $f(x) \sqsubseteq f(y)$. Therefore if $U \subset D'$ is open, so is $f^{-1}(U) \subset D$. $\square$

4.4. DEFINITION. If $f(\sqcup X) = \sqcup f(X)$ holds for arbitrary X , then f is called *distributive*.

4.5. COROLLARY. Let $f_i : D \rightarrow D'$ be a collection of continuous mappings. Define $f = \lambda x. \sqcup_i f_i(x)$. Then f is continuous.

PROOF. $f(\sqcup X) = \sqcup_i \sqcup_{x \in X} f_i(x) = \sqcup_{x \in X} \sqcup_i f_i(x) = \sqcup f(X)$. $\square$

4.6. DEFINITION. $D \times D'$ is the cartesian product partially ordered by $\langle x, x' \rangle \sqsubseteq \langle y, y' \rangle$ iff $x \sqsubseteq x'$ and $y \sqsubseteq y'$. $[D \rightarrow D']$ is the set of continuous maps $\in D \rightarrow D'$ partially ordered by $f \sqsubseteq g \Leftrightarrow \forall x \in D \ f(x) \sqsubseteq g(x)$. Then $D \times D'$ and $[D \rightarrow D']$ are complete lattices with $\sqcup X = \langle \sqcup (X)_0, \sqcup (X)_1 \rangle$ for $X \subset D \times D'$ and $\sqcup F = \lambda x. \sqcup \{f(x) \mid f \in F\}$ for $F \subset [D \rightarrow D']$. (If $z = \langle x, y \rangle$, $z_0 = x$, $z_1 = y$; $\sqcup F$ is continuous by 4.5.) The induced topology on $D \times D'$ is not necessarily the product of the induced topologies on D and D' .

4.7. LEMMA. $f : D \times D' \rightarrow D''$ is continuous $\Leftrightarrow f$ is continuous in each of its variables separately (i.e. $\lambda d. f(d, d'_0)$ and $\lambda d'. f(d_0, d')$ are continuous for all d_0, d'_0).

PROOF. ($\Rightarrow$) As ever.

$$(\Leftarrow) f(\sqcup X) = f(\sqcup X_0, \sqcup X_1)$$

$$= \sqcup_{d \in X_0} f(d, \sqcup X_1) = \sqcup_{d \in X_0} \sqcup_{d' \in X_1} f(d, d') = \sqcup_{\langle d, d' \rangle \in X} f(d, d') = \sqcup f(X). \quad \square$$

4.8. LEMMA (Continuity of application). *Define Ap (application) $[D \rightarrow D'] \times D \rightarrow D'$ by $\text{Ap}(f, x) = f(x)$. Then Ap is continuous.*

PROOF. $\lambda x. f_0(x) = f_0$ is continuous. $\lambda f. f(x_0) = h_0$ with $h_0(\sqcup F) = \sqcup F(x_0) = \sqcup_{f \in F} f(x_0) = \sqcup h_0(F)$. Hence h_0 is continuous. Therefore, by 4.7, Ap is continuous. $\square$

4.9. LEMMA (Continuity of abstraction). *Let $f \in [D \times D' \rightarrow D'']$. Define $g_f(x) = \lambda y \in D'. f(x, y)$. Then*

- (i) g_f is continuous,
- (ii) $\lambda f. g_f : [D \times D' \rightarrow D''] \rightarrow [D \rightarrow [D' \rightarrow D'']]$ is continuous.

PROOF. (i) $g_f(\sqcup X) = \lambda y. f(\sqcup X, y) = \lambda y. \sqcup_{x \in X} f(x, y) = \sqcup_{x \in X} \lambda y. f(x, y) = \sqcup g_f(X)$. ($\lambda y. \sqcup = \sqcup \lambda y$ follows from the definition of $\sqcup$ in a function space.)

(ii) Let $L = \lambda f. g_f$. $L(\sqcup F) = \lambda x. \lambda y. \sqcup_{f \in F} f(x, y) = \sqcup_{f \in F} \lambda x. \lambda y. f(x, y) = \sqcup L(F)$. $\square$

4.10. DEFINITION. Let $\phi : D \rightarrow D'$, $\psi : D' \rightarrow D$. $\langle \phi, \psi \rangle$ is a *projection* of D on D' iff

- (i) ϕ, ψ are continuous,
- (ii) $\forall x \in D \psi(\phi(x)) = x$,
- (iii) $\forall x \in D' \phi(\psi(x)) \sqsubseteq x$.

4.11. DEFINITION (Construction of D_∞). Let D be an arbitrary nontrivial complete lattice. Define $D_0 = D$, $D_{n+1} = [D_n \rightarrow D_n]$. Mappings $\phi_n : D_n \rightarrow D_{n+1}$ and $\psi_n : D_{n+1} \rightarrow D_n$ are defined as follows:

$$\phi_0(x) = \lambda y \in D_0. x, \quad \psi_0(x') = x'(\perp), \quad \text{where } \perp \in D_0.$$

$$\phi_{n+1}(x) = \phi_n \circ x \circ \psi_n, \quad \psi_{n+1}(x') = \psi_n \circ x' \circ \phi_n \quad (\text{see Diagram 1}).$$

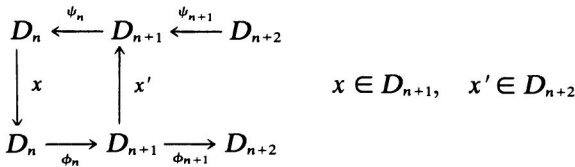


Diagram 1.

By a straightforward induction on n it follows that $\langle \phi_n, \psi_n \rangle$ is a projection of D_{n+1} on D_n . Moreover ϕ_n and ψ_n are distributive. For an element $x = \langle x_n \rangle_{n=0}^\infty$ of the product $\prod_{n=0}^\infty D_n$, x_i denotes the i -th coordinate,

$$D_\infty = \varprojlim (D_n, \psi_n) = \left\{ x \in \prod_n D_n \mid \forall n \in \omega \psi_n(x_{n+1}) = x_n \right\}.$$

For $x, y \in D_\infty$, a partial ordering is defined by $x \sqsubseteq y \Leftrightarrow \forall n \in \omega x_n \sqsubseteq y_n$. Then D_∞ is a complete lattice with for $X \subset D_\infty$, $\sqcup X = \langle \sqcup X_n \rangle_{n=0}^\infty$. This belongs to D_∞ since $\psi_n(\sqcup X_{n+1}) = \sqcup \psi_n(X_{n+1}) = \sqcup X_n$, by the distributivity of ψ_n .

4.12. DEFINITION. Mappings $\Phi_{n,m} : D_n \rightarrow D_m$ are defined (by following the arrows in $D_0 \rightrightarrows D_1 \rightrightarrows \dots$). If $n \leq m$, say $m = n + k$, Φ_{nm} is defined by induction on k . $\Phi_{nn} = \lambda x \in D_n. x$. $\Phi_{n(m+1)} = \phi_m \circ \Phi_{nm}$. If $m \leq n$, say $n = m + k$, Φ_{nm} is again defined by induction k : $\Phi_{(n+1)m} = \Phi_{nm} \circ \psi_n$.

$\Phi_{n\infty} : D_n \rightarrow D_\infty$ is defined by $\Phi_{n\infty}(x) = \langle \Phi_{ni}(x) \rangle_{i=0}^\infty$. $\Phi_{\infty n} : D_\infty \rightarrow D_n$ is defined by $\Phi_{\infty n}(x) = x_n$.

4.13. LEMMA. (i) For $0 \leq n \leq m \leq \infty$, $\langle \Phi_{nm}, \Phi_{mn} \rangle$ is a projection of D_n on D_m .
(ii) For $0 \leq n \leq m \leq l \leq \infty$, $\Phi_{ml} \circ \Phi_{nm} = \Phi_{nl}$.

PROOF. Standard. $\square$

It follows that up to isomorphism $D_0 \subseteq D_1 \subseteq \dots \subseteq D_\infty$. In fact in the category of *complete* lattices with continuous mappings as morphisms, D_∞ is not only the inverse limit $\varprojlim (D_n, \psi_n)$, but also a direct limit: $D_\infty = \varinjlim (D_n, \phi_n)$. Note however $D_\infty \neq \bigcup_n D_n$, D_∞ is the completion of $\bigcup D_n$. Henceforth each element $x \in D_n$ will be identified with $\Phi_{n\infty}(x) \in D_\infty$, as is customary with direct limits. In particular

4.14. LEMMA. (i) If $x \in D_n$, then $x = x_n$.

(ii) If $x \in D_n$, then $\phi_n(x) = x$.

(iii) If $x \in D_{n+1}$, then $\psi_n(x) \sqsubseteq x$.

PROOF. (i) x in D_∞ is $\langle \dots, \psi(x), x, \phi(x), \phi(\phi(x)), \dots \rangle$. Hence x_n is x .

(ii) $\phi_n(x)$ in D_∞ is $\langle \dots, \psi(\phi_n(x)), \phi_n(x), \phi(\phi_n(x)), \dots \rangle$. Since $\psi(\phi(x)) = x$, this is the same as x in D_∞ .

(iii) Analogous, using $\phi(\psi(x)) \sqsubseteq x$. $\square$

Due to the identifications, properties of D_∞ are more elegant to formulate:

4.15. LEMMA. In D_∞

- (i) $(x_n)_m = x_{\min(n, m)}$.
- (ii) If $n \leq m$, then $x_n \sqsubseteq x_m \sqsubseteq x$.
- (iii) $x = \bigsqcup_{n=0}^{\infty} x_n$.
- (iv) $\top_n$ and $\perp_n$ are top and bottom of D_n .
- (v) $\perp_n = \perp$; $\top_n = \top$.

PROOF. (i) If $m \leq n$, $(x_n)_m = \Phi_{nm}x_n = \psi \circ \dots \circ \psi(x_n) = x_m$, since $x \in D_{\infty}$. If $m \geq n$, $(x_n)_m = \phi \circ \dots \circ \phi(x_n) = x_n$ by 4.14(ii).

(ii) First, by 4.14(iii), $x_m \sqsubseteq x_{m+1}$, since $x_m = \psi_m(x_{m+1})$. Hence $x_0 \sqsubseteq x_1 \sqsubseteq \dots$. Furthermore $x_n \sqsubseteq x$ since $\forall i (x_n)_i = x_{\min(n, i)} \sqsubseteq x_i$.

(iii) $\bigsqcup_n x_n = \langle \bigsqcup_n (x_n)_i \rangle_{i=0}^{\infty} = \langle \bigsqcup_n x_{\min(n, i)} \rangle_{i=0}^{\infty} = \langle x_i \rangle_{i=0}^{\infty} = x$.

(iv) Let $\top'_n$ and $\perp'_n$ be resp. top and bottom of D_n . Then

$$\top = \bigsqcup D_{\infty} = \langle \bigsqcup D_n \rangle_{n=0}^{\infty} = \langle \top'_n \rangle_{n=0}^{\infty}$$

and

$$\perp = \bigsqcup \emptyset = \langle \bigsqcup \emptyset \rangle_{n=0}^{\infty} = \langle \perp'_n \rangle_{n=0}^{\infty}.$$

Hence $\top_n = \top'_n$, $\perp_n = \perp'_n$.

(v) By (ii), $\perp_n \sqsubseteq \perp$ and $\perp \sqsubseteq \perp_n$ always. So $\perp_n = \perp$. On the other hand it follows by induction that $\phi_n(\top_n) = \top_{n+1}$, since $\top_{n+1} = \lambda x \in D_n. \top_n$. Moreover since $\langle \top_n \rangle_{n \in \omega} \in D_{\infty}$, $\psi_n(\top_{n+1}) = \top_n$. Therefore $\top_n$ in D_{∞} , i.e., $\langle \Phi_{nm}(\top_n) \rangle_{m \in \omega}$ is $\langle \top_m \rangle_{m \in \omega} = \top$. $\square$

4.16. DEFINITION. In D_{∞} one can define a binary operation application: $x \cdot y = \bigsqcup_n x_{n+1}(y_n)$. On the RHS the application is the usual one $D_{n+1} \times D_n \rightarrow D_n$ and the $\bigsqcup$ is to be taken in D_{∞} after identification.

4.17. LEMMA. *Application is well defined, in the sense that if $x_{n+1} \in D_{n+1}$ and $y_n \in D_n$, then $x_{n+1} \cdot y_n = x_{n+1}(y_n)$.*

PROOF.

$$\begin{aligned} x_{n+1} \cdot y_n &= \bigsqcup_{i=0}^{\infty} (x_{n+1})_{i+1}((y_n)_i) \\ &= \bigsqcup_{i=0}^n x_{i+1}(y_i) \quad \text{by 4.15(i),} \\ &= x_{n+1}(y_n) \quad \text{by 4.15(ii).} \quad \square \end{aligned}$$

4.18. LEMMA. *Application is continuous.*

PROOF. $x \cdot y = \bigsqcup_n \Phi_{n\infty}(x_{n+1}(y_n))$. Now apply 4.5, 4.8 and 4.13. $\square$

4.19. LEMMA. (i) $x_{n+1} \cdot y = x_{n+1} \cdot y_n = (x \cdot y_n)_n$.

(ii) $x_0 \cdot y = x_0 = (x \cdot \perp)_0$.

PROOF. (i) First it is shown by induction on $i \geq n$ that $(x_{n+1})_{i+1}(y_i) = x_{n+1}(y_n)$. For $i = n$ this is clear. Now

$$\begin{aligned} (x_{n+1})_{i+2}(y_{i+1}) &= \phi_{i+1}((x_{n+1})_{i+1})(y_{i+1}) = \phi_i \circ (x_{n+1})_{i+1} \circ \psi_i(y_{i+1}) \\ &= \phi_i((x_{n+1})_{i+1}(y_i)) = (x_{n+1})_{i+1}(y_i), \quad \text{by 4.14(ii),} \\ &= x_{n+1}(y_n) \end{aligned}$$

by the induction hypothesis. Therefore

$$\begin{aligned} x_{n+1} \cdot y &= \bigsqcup_{i=n}^{\infty} (x_{n+1})_{i+1}(y_i) \\ &= \bigsqcup_{i=n}^{\infty} x_{n+1}(y_n) = x_{n+1} \cdot y_n \quad (\text{by 4.17}). \end{aligned}$$

Again by induction on $i \geq n$ it is shown that $(x_{i+1}(y_n))_i = x_{n+1}(y_n)$. For $i = n$ this is clear. Now

$$\begin{aligned} (x_{i+2}(y_n)_{i+1})_n &= \Phi_{i+1n}(x_{i+2}(\phi_i((y_n)_i))) = \Phi_{in} \circ \psi_i \circ x_{i+2}(\phi_i((y_n)_i)) \\ &= \Phi_{in}((\psi_{i+1}(x_{i+2}))(y_n)_i) = \Phi_{in}(x_{i+1}(y_n)_i) \\ &= (x_{i+1}(y_n)_i)_n = x_{n+1}(y_n) \end{aligned}$$

by the induction hypothesis. Therefore

$$(x \cdot y_n)_n = \left(\bigsqcup_i x_{i+1}((y_n)_i) \right)_n = \bigsqcup_i (x_{i+1}((y_n)_i))_n = \bigsqcup_i x_{n+1}(y_n) = x_{n+1} \cdot y_n.$$

(ii) By (i), $x_0 \cdot y = (x_0)_1 \cdot y = (x_0)_1(y_0) = \phi_0(x_0)(y_0) = x_0$. Also $x_0 = \psi_0(x_1) = x_1(\perp_0) = (x \cdot \perp)_0 = (x \cdot \perp)_0$. $\square$

4.20. THEOREM (extensionality). For $x, y \in D_\infty$,

(i) $x \sqsubseteq y \Leftrightarrow \forall z \in D_\infty x \cdot z \sqsubseteq y \cdot z$,

(ii) $x = y \Leftrightarrow \forall z \in D_\infty x \cdot z = y \cdot z$.

PROOF. (i) $(\Rightarrow)$ By monotonicity of $\lambda x(x \cdot z)$. $(\Leftarrow)$ Suppose $\forall z x \cdot z \sqsubseteq y \cdot z$. Then $x \cdot \perp \sqsubseteq y \cdot \perp$, so $x_0 = (x \cdot \perp)_0 \sqsubseteq (y \cdot \perp)_0 = y_0$ by 4.19(ii). Moreover $x \cdot z_n \sqsubseteq y \cdot z_n$, so $x_{n+1}(z_n) = (x \cdot z_n)_n \sqsubseteq (y \cdot z_n)_n = y_{n+1}(z_n)$ by 4.17 and 4.19(i). Hence $x_{n+1} \sqsubseteq y_{n+1}$. Now we have $\forall n x_n \sqsubseteq y_n$, i.e. $x \sqsubseteq y$.

(ii) Immediate by (i). $\square$

4.21. THEOREM (completeness). $\forall f \in [D_\infty \rightarrow D_\infty] \exists x \in D_\infty f(y) = x \cdot y$.

PROOF. Let $x = \bigsqcup_n (\lambda y \in D_n \cdot (f(y))_n)$. Note that this is the supremum of a directed set. Remark that for a_{ij} in a complete lattice,

$$\bigsqcup_{i,j} a_{ij} = \bigsqcup_k a_{kk} \quad \text{if } \forall i, j \exists k a_{ij} \sqsubseteq a_{kk}.$$

Now

$$\begin{aligned} x \cdot y &= \bigsqcup_m x_{m+1}(y_m) = \bigsqcup_m (x \cdot y_m)_m = \bigsqcup_m \left(\left(\bigsqcup_n \lambda y \in D_n \cdot (f(y))_n \right) \cdot y_m \right)_m \\ &= \bigsqcup_{m,n} (\lambda y \in D_n (f(y))_n \cdot y_m)_m = \bigsqcup_m (\lambda y \in D_m (f(y))_m \cdot y_m) \\ &= \bigsqcup_m (f(y_m))_m = \bigsqcup_{k,l} (f(y_k))_l = \bigsqcup_k f(y_k) = f(y). \end{aligned}$$

Comments that should accompany these equations follow easily from the continuity (monotonicity) of the functions involved and the remark above. $\square$

4.22. COROLLARY. D_∞ is homeomorphic to $[D_\infty \rightarrow D_\infty]$.

PROOF. For $x \in D_\infty$ let $F(x) = \lambda y \in D_\infty x \cdot y$. F is surjective by 4.21, injective by 4.20, continuous by 4.9(i). The inverse to F is, by the proof of 4.21, $\lambda f \bigsqcup_n (\lambda y \in D_n (f(y))_n)$ which is continuous by 4.9(ii) and 4.5. $\square$

4.23. THEOREM. D_∞ is an extensional λ -algebra.

PROOF. Combinatory completeness follows from 4.21 since application and abstraction are continuous. Extensionality was proved in 4.20(ii). Hence 1.16(2) applies. $\square$

Since D_∞ is extensional there is no ambiguity interpreting λ -terms in it. However for later reference, the interpretation will be given explicitly.

4.24. DEFINITION. (i) A valuation (in D_∞) is a mapping ρ : variables $\rightarrow D_\infty$.

(ii) For $d \in D_\infty$ and x a variable, $\rho(d/x)$ is the valuation ρ' with $\rho'(y) = d$ if $y = x$ then $\rho(y)$ else d .

(iii) The interpretation of M in D_∞ under ρ , $\llbracket M \rrbracket \rho$, is defined inductively: $\llbracket x \rrbracket \rho = \rho(x)$, $\llbracket MN \rrbracket \rho = \llbracket M \rrbracket \rho \llbracket N \rrbracket \rho$, $\llbracket \lambda x. M \rrbracket \rho = \lambda d. \llbracket M \rrbracket \rho(d/x) \in D_\infty$ after identification with $[D_\infty \rightarrow D_\infty]$.

Roughly, in the interpretation formal variables are replaced by variables

ranging over D_∞ and application and abstraction are to be taken in D_∞ . From this it should be obvious that the interpretation is correct. This can be made precise by showing inductively $\llbracket (\lambda x M) N \rrbracket \rho = \llbracket M \rrbracket \rho (\llbracket N \rrbracket \rho / x) = \llbracket M(x/N) \rrbracket \rho$.

Whenever possible the valuation ρ will be omitted in the notation $\llbracket M \rrbracket \rho$.

5. Solvability

The concept of solvability and the related notion of head normal form were introduced respectively in the dissertations of Barendregt and Wadsworth. Both theses give arguments for the computational irrelevance of unsolvable terms. Therefore a λ -theory (or λ -algebra) is called *sensible* iff it equates all unsolvable terms. It turned out that there is a unique maximal sensible theory. In Section 7 it will be proved that this theory equals $\text{Th}(D_\infty)$.

5.1. DEFINITION. (i) A closed term M is *solvable* iff $\lambda \vdash MN_1 \cdots N_n = I$ for some n and terms $N_1 \cdots N_n$.

(ii) An arbitrary term M is solvable iff its closure $\lambda \vec{x}. M$ is solvable. M is *unsolvable* iff M is not solvable.

(iii) $\mathcal{H} = \{M = N \mid M, N \text{ unsolvable}\}$.

To see the particular role of I in this definition, note that M (closed) is solvable iff $\forall P \exists \vec{N} M\vec{N} = P$.

5.2. DEFINITION. (i) Each λ -term M is of the form

$$\lambda x_1 \cdots x_n. (\lambda x. P) Q M_1 \cdots M_m \quad \text{or} \quad \lambda x_1 \cdots x_n. x_i M_1 \cdots M_m,$$

$m, n \geq 0$. In the first case $(\lambda x. P)Q$ is the *head redex* of M . In the second case x_i is the *head variable* of M and M is said to be in *head normal form* (hnf).

The following can be proved syntactically. A semantic proof will be given in 7.9 and 7.10.

5.3. THEOREM. (i) M is solvable $\Leftrightarrow M$ has a hnf.

(ii) $\lambda\eta + \mathcal{H}$ is consistent.

5.4. EXAMPLES. I and Y are solvable; Ω and $K^\infty \equiv YK$ are unsolvable

(note that $\lambda \vdash Y(KI) = I$, $\Omega N_1 \cdots N_n \rightarrow M \Rightarrow M \equiv \Omega N'_1 \cdots N'_n$ with $N_i \rightarrow N'_i$, and $\lambda \vdash K^\infty M = K^\infty$ for all M). Note also $\lambda + \mathcal{H} \vdash \lambda x. \Omega = \Omega x = \Omega$, since M unsolvable $\Rightarrow MN, \lambda x. M$ unsolvable.

5.5. DEFINITION. (i) A context $C[\cdot]$ is a term with some holes in it. More formally: any variable x is a context; $[\cdot]$ is a context; if $C_1[\cdot], C_2[\cdot]$ are contexts, so are $(C_1[\cdot] C_2[\cdot])$ and $(\lambda x. C[\cdot])$. If M is an arbitrary term and $C[\cdot]$ a context, $C[M]$ denotes the result of placing M in the holes of $C[\cdot]$. In this act, free variables of M may become bound in $C[M]$.

(ii) M and N are *solvably equivalent*, notation $M \sim_s N$ iff $\forall C[\cdot] [C[M]$ is solvable $\Leftrightarrow C[N]$ is solvable].

(iii) $\mathcal{H}^* = \{M = N \mid M, N \in \Lambda^0 \text{ and } M \sim_s N\}$.

5.6. LEMMA. $\mathcal{H}^* = \mathcal{H}^{**}$.

PROOF. Induction on the length of proof shows that $\lambda + \mathcal{H}^* \vdash M = N \Rightarrow M \sim_s N$. $\square$

5.7. COROLLARY. $\mathcal{H}^*$ is consistent hence a λ -theory.

PROOF. $I \not\sim_s \Omega$, hence $I = \Omega \notin \mathcal{H}^*$. $\square$

5.8. LEMMA. If $\mathcal{H} + M = N$ is consistent, then $\mathcal{H}^* \vdash M = N$.

PROOF. First note that $\{I = K^\infty\}$ is inconsistent: $\lambda + I = K^\infty \vdash M = IM = K^\infty M = K^\infty$ for all M . Now suppose $M = N \notin \mathcal{H}^*$. Then, say, $C[M]$ is solvable and $C[N]$ is unsolvable for some $C[\cdot]$. Therefore $\lambda \vdash (\lambda \vec{x}. C[M])\vec{P} = I$ for some $\vec{P}$ and $\mathcal{H} \vdash C[N] = K^\infty$. Now

$$\begin{aligned} \lambda + \mathcal{H} + M = N \vdash I &= (\lambda \vec{x}. C[M])\vec{P} = (\lambda \vec{x}. C[N])\vec{P} \\ &= (\lambda \vec{x}. K^\infty)\vec{P} = K^\infty \vec{P} = K^\infty, \end{aligned}$$

so $\lambda + \mathcal{H} + M = N$ would be inconsistent. $\square$

5.9. COROLLARY. (i) $\mathcal{H}^*$ is the unique maximal λ -theory extending $\mathcal{H}$.

(ii) Moreover, $\mathcal{H}^*$ proves extensionality.

PROOF. (i) Since $\text{Con}(\mathcal{H})$, by 5.3, $\mathcal{H} \subset \mathcal{H}^*$ by 5.8. If T is a consistent extension of $\mathcal{H}$, then for each $M = N \in T$, $M = N \in \mathcal{H}^*$ by 5.8; so $T \subset \mathcal{H}^*$.

Therefore $\mathcal{H}^*$ contains each consistent extension of $\mathcal{H}$ and being itself consistent, 5.7, the statement follows.

(ii) $\lambda + \mathcal{H} + (\lambda x. Mx) = M$ ($x \notin \text{FV}(M)$) is consistent by 5.3(ii). Hence $\mathcal{H}^* \vdash \lambda x. Mx = M$. $\square$

The possibility that $\mathcal{H}$ has a *unique* maximally consistent extension is due to the fact that the language of the λ -calculus is logic free, i.e. it is not possible that for an undecided sentence σ we make two extensions by adding σ and $\neg\sigma$ respectively, because the language does not contain negation. The theory λ however has $2^{\aleph_0}$ maximal consistent extensions.

5.10. DEFINITION. A λ -algebra $\mathfrak{M}$ is *sensible* iff $\mathfrak{M} \models \mathcal{H}$. In that case $\text{Th}(\mathfrak{M}) \subset \mathcal{H}^*$ by 5.9.

The “least” sensible model is $\mathfrak{M}^0(\mathcal{H}^*)$:

5.11. COROLLARY. $\mathfrak{M}^0(\mathcal{H}^*)$ is *algebraically simple*, i.e. has no proper homomorphic images.

PROOF. If $\mathfrak{M}$ were a proper image of $\mathfrak{M}^0(\mathcal{H}^*)$, then $\text{Th}(\mathfrak{M})$ would be a proper extension of $\mathcal{H}^*$. $\square$

In Section 7 it will be shown that $\mathfrak{M}^0(\mathcal{H}^*)$ is the interior of D_∞ .

6. Böhm trees

The trees introduced in this section are inspired by the proof of the Theorem of Böhm, 2.23, and the concept of solvability. The Böhm trees are useful for the analysis of $\mathcal{P}\omega$ and D_∞ . See NAKAJIMA [1975] for a related family of trees.

6.1. DEFINITION. A *tree* is a set A of sequence numbers such that

- (i) if $\alpha \in A$ and $\beta < \alpha$ (ordering of sequence numbers), then $\beta \in A$,
- (ii) for each $\alpha \in A$ there are only finitely many immediate successors of α in A . The $\alpha \in A$ are called the *nodes* of the tree. The depth of $\alpha = \langle n_0, \dots, n_{k-1} \rangle$, notation $d(\alpha)$, is k . $*$ denotes concatenation, i.e. $\langle \vec{n} \rangle * \langle \vec{m} \rangle = \langle \vec{n}, \vec{m} \rangle$. Then *subtree* at α of A , A_α , is the set $\{\beta \mid \alpha * \beta \in A\}$.

6.2. DEFINITION. (i) A *labelled tree* is a tree where at each node there is a

symbol which is either Ω or $\lambda x_1 \cdots x_n. x_i$ for some variables $x_1, \dots, x_n, x_i$. To be precise, a labelled tree is a mapping f_A from the sequence numbers into the set

$$\{*, \Omega\} \cup \{\langle i_1, \dots, i_n \rangle, i \mid i, n, i_1, \dots, i_n \in \omega\},$$

such that $A = \{\alpha \mid f_A(\alpha) = *\}$ is a tree. $f_A(\alpha) = \langle i_1, \dots, i_n \rangle, i$ (resp. Ω) means that $\lambda a_{i_1} \cdots a_{i_n}. a_i$ (resp. Ω) is written at node $\alpha \in A$.

(ii) If A, B are labelled trees, then

$$A \equiv_k B \Leftrightarrow \forall \alpha \left[[d(\alpha) < k \Rightarrow f_A(\alpha) = f_B(\alpha)] \wedge \right. \\ \left. \wedge [d(\alpha) = k \Rightarrow f_A(\alpha) \neq * \Leftrightarrow f_B(\alpha) \neq *]] \right].$$

i.e. for depth $< k$ the labelled trees are equal and the nodes of depth $k - 1$ have in both trees the same number of successors.

6.3. DEFINITION. The *Böhm tree* of a λ -term M , $BT(M)$, is a labelled tree defined as follows: If m is unsolvable, then $BT(M) = \Omega$. If M is solvable, say M has hnf $\lambda x_1 \cdots x_n. x_i M_1 \cdots M_m$, then $BT(M)$ is

$$\lambda x_1 \cdots x_n. x_i \overbrace{BT(M_1) \cdots BT(M_m)} \quad .$$

To be precise, if M is unsolvable, then $BT(M)(\langle \cdot \rangle) = \Omega$, $BT(M)(\langle j \rangle * \alpha) = *$. If M is solvable, say M has hnf $\lambda a_{i_1} \cdots a_{i_n}. a_i M_0 \cdots M_{m-1}$, then $BT(M)(\langle \cdot \rangle) = \langle i_1, \dots, i_n \rangle, i$, $BT(M)(\langle j \rangle * \alpha) = BT(M_j)(\alpha)$, for $j < m$ and $BT(M)(\langle j \rangle * \alpha) = *$ for $j \geq m$.

Free and bound occurrences of a variable in a Böhm tree are defined as for terms. As with terms, Böhm trees are considered modulo a change of bound variables.

From the Church–Rosser theorem it follows that if M has a hnf $\lambda x_1 \cdots x_n. x_i M_1 \cdots M_m$, then n, i, m are uniquely determined. Hence the Böhm tree of M is well defined and if $\lambda \vdash M = N$, then $BT(M) = BT(N)$.

6.4. EXAMPLE.

$$\begin{array}{llll} BT(S): & \lambda abc. a. & BT(Sx\Omega): & \lambda x. x. \\ & \begin{array}{c} \diagup \quad \diagdown \\ c \quad b \\ | \\ c \end{array} & & \begin{array}{c} \diagup \quad \diagdown \\ c \quad \Omega \end{array} \\ & & & BT(Y): & \lambda f. f. \\ & & & & \begin{array}{c} | \\ f \\ | \\ \vdots \end{array} \end{array}$$

Note that although $\lambda x.x$ and $\lambda xy.xy$ are extensionally equal, they have different Böhm trees. Therefore the following equivalence relation is introduced.

6.5. DEFINITION. (i) M', N' *merge* $\text{BT}(M), \text{BT}(N)$ *up to* k iff $\lambda\eta \vdash M = M', \lambda\eta \vdash N = N'$ and $\text{BT}(M') \equiv_k \text{BT}(N')$.

(ii) M, N have *equivalent* Böhm trees, notation $\text{BT}(M) \sim_\eta \text{BT}(N)$, iff $\forall k \exists M', N' \ M', N'$ merge $\text{BT}(M), \text{BT}(N)$ up to k .

Now we give some examples of terms with equal or equivalent Böhm trees.

6.6. Example. (i) By the fixed point theorem there exists a term A such that $Ax \rightarrow \lambda z.z(Ax)$. Then $\text{BT}(Ax) = \text{BT}(Ay)$ (x and y disappear from the tree).

(ii) Let $Y_z = \lambda f.(\lambda xz.f(xxz))(\lambda xz.f(xxz))z$. Then Y_z is an alternative fixed point operator not convertible with Y . But $\text{BT}(Y_z) = \text{BT}(Y)$.

(iii) $\text{BT}(\lambda x.x) \sim_\eta \text{BT}(\lambda xy.xy)$.

The following is a less trivial example of equivalent Böhm trees. Together with the characterization Theorem 7.1 it shows that in D_∞ a normal form may be equal to a term without a nf.

6.7. EXAMPLE (Wadsworth). Let $J = Y(\lambda jxy.x(jy))$. Then $\text{BT}(J) \sim_\eta \text{BT}(I)$.

PROOF. The hnf of J is $\lambda x_0 x_1. x_0(Jx_1)$, so $\text{BT}(J)$ is

$$\begin{array}{c} \lambda x_0 x_1. x_0 \\ | \\ \lambda x_2. x_1 \\ | \\ \lambda x_3. x_2 \\ | \\ \vdots \end{array}$$

This can be merged to any depth with $\text{BT}(I)$ by some η expansions (i.e. the opposite of a contraction) of the latter. $\square$

6.8. THEOREM. $\mathcal{H}^* \vdash M = N \Rightarrow \text{BT}(M) \sim_\eta \text{BT}(N)$.

The rather technical proof occupies the rest of this section and can be omitted at a first reading.

6.9. DEFINITION. Let A, A' be Böhm trees.

(i) A, A' are *top mergeable* iff either A, A' are both Ω or A and A' are

$$\begin{array}{cc} \lambda x_1 \cdots x_n \cdot x_i & \lambda x_1 \cdots x_{n'} \cdot x_{i'} \\ \swarrow \quad \searrow & \swarrow \quad \searrow \\ \square_1 \cdots \square_m & \square'_1 \cdots \square'_{m'} \end{array}$$

respectively, and $i = i'$ and $n - m = n' - m'$ (possibly negative numbers); the sequences $x_1, \dots, x_n$ and $x_1, \dots, x_{n'}$ can be assumed to start similarly, by a change of bound variables.

(ii) Let α be a common node of A, A' . A, A' are *mergeable at α* iff A_α, A'_α are top mergeable.

(iii) A, A' *separate at depth k* iff $A \equiv_k A'$ and A, A' are not mergeable at some common node α with $d(\alpha) = k$.

6.10. LEMMA. Let $BT(M) \equiv_k BT(N)$. If $BT(M), BT(N)$ are mergeable at all α with $d(\alpha) = k$, then they can be merged up to $k + 1$.

PROOF. Let $d(\alpha) = k$. $BT(M)_\alpha, BT(N)_\alpha$ are, say,

$$\begin{array}{cc} \lambda x_1 \cdots x_n \cdot x_i & \text{and} \quad \lambda x_1 \cdots x_{n'} \cdot x_{i'} \\ \swarrow \quad \searrow & \swarrow \quad \searrow \\ \square_1 \cdots \square_m & \square'_1 \cdots \square'_{m'} \end{array}$$

Now make an η -change as follows

$$\begin{array}{cc} \lambda x_1 \cdots x_n x_{n+1} \cdots x_{n+n'} \cdot x_i & \lambda x_1 \cdots x_n x_{n'+1} \cdots x_{n'+n} \cdot x_i \\ \swarrow \quad \downarrow \quad \searrow & \swarrow \quad \downarrow \quad \searrow \\ \square_1 \cdots \square_m x_{n+1} \cdots x_{n+n'} & \square'_1 \cdots \square'_{m'} x_{n'+1} \cdots x_{n'+n} \end{array}$$

Note that $m + n' = m' + n$ by the mergeability at α , so after the change, α has the same number of successors in both trees. After this change is made for all α with $d(\alpha) = k$, the resulting labelled trees are Böhm trees of M', N' , say, which merge $BT(M), BT(N)$ up to $k + 1$. $\square$

6.11. COROLLARY. If $BT(M) \not\equiv_\eta BT(N)$, then $\exists k, M', N'$ such that M', N' merge $BT(M), BT(N)$ up to k and $BT(M'), BT(N')$ separate at depth k .

PROOF. Let k be maximal such that $BT(M), BT(N)$ can be merged up to k , by some M', N' . Then $BT(M') \equiv_k BT(N')$. Suppose that $BT(M'), BT(N')$

are mergeable at all α with $d(\alpha) = k$. Then by 6.10, $\text{BT}(M')$, $\text{BT}(N')$, and hence $\text{BT}(M)$, $\text{BT}(N)$, can be merged up to $k + 1$, contradicting the maximality of k . Therefore $\text{BT}(M')$, $\text{BT}(N')$ separate at depth k . $\square$

6.12. DEFINITION. (i) A *transformation* is a mapping $f : \Lambda \rightarrow \Lambda$.

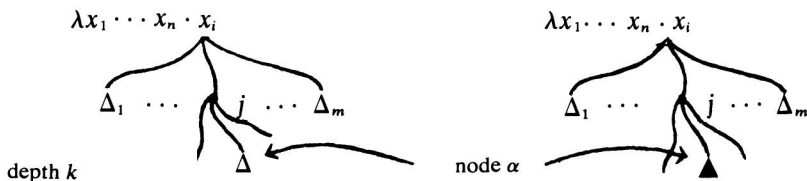
(ii) A *solving transformation* f is either defined by $f(P) = Px$ for some x or by $f(P) = P[x/Nx]$ for some x and closed N .

(iii) A *Böhm transformation* is a finite composition of solving transformations. Notations: π ranges over Böhm transformations; $M^\pi = \pi(M)$.

6.13. DEFINITION. $\text{BT}(M)$ is *head original* up to k iff $\text{BT}(M)$ has a free head variable which does not occur freely at any other node α with $d(\alpha) \leq k$.

6.14. LEMMA. If $\text{BT}(M)$, $\text{BT}(N)$ are head original up to k and separate at depth $k > 0$, then for some π , $\text{BT}(M^\pi)$, $\text{BT}(N^\pi)$ separate at depth $k - 1$.

PROOF. Let the trees separate at node α :



Define $\pi(P) = Px_1 \cdots x_n [x_i / U_j^m x_i]$, where $U_j^m = \lambda y_1 \cdots y_m \cdot y_j$. Then $\text{BT}(M^\pi)$, $\text{BT}(N^\pi)$ separate at depth $k - 1$:



The assumption of head originality is needed to insure that the difference Δ , $\blacktriangle$ is not lost by the substitution $[x_i / U_j^m x_i]$. $\square$

6.15. LEMMA. Let $\text{BT}(M)$, $\text{BT}(N)$ separate at depth $k > 0$. Then for some π , $\text{BT}(M^\pi)$ are head original up to k and still separate at depth k .

PROOF. Let $C_q = \lambda z_0 \cdots z_{q+1} \cdot z_{q+1} z_0 \cdots z_q$. For a node α in a Böhm tree let $\# \alpha$ be $\max(s, t)$ where $\lambda a_1 \cdots a_{i_s} \cdot a_j$ is the label at α and t is the number of successors of α ; $\# \alpha$ is 0 if Ω is the label at α . The assumption implies that

M, N have hnf's, say $\lambda x_1 \cdots x_n. x_i M_1 \cdots M_m$ and $\lambda x_1 \cdots x_n. x_i N_1 \cdots N_m$ respectively. Now define

$$\pi(P) = (Px_1 \cdots x_n)[x_i/C_q x_i]z_{m+1} \cdots z_{q+1},$$

where $q > 2(\# \alpha)$ for all α in $\text{BT}(M)$, $\text{BT}(N)$ with $d(\alpha) \leq k$ and $z_{m+1} \cdots z_{q+1}$ are fresh variables. Note that the Böhm trees at depth $\leq k$ of M^π, N^π result from those of M, N respectively by replacing the tops

$$\lambda x_1 \cdots x_n. x_i \quad \text{by} \quad \begin{array}{c} z_{q+1} \\ \swarrow \quad \downarrow \quad \searrow \\ x_i \square_1 \cdots \square_m z_{m+1} \cdots z_q \end{array}$$

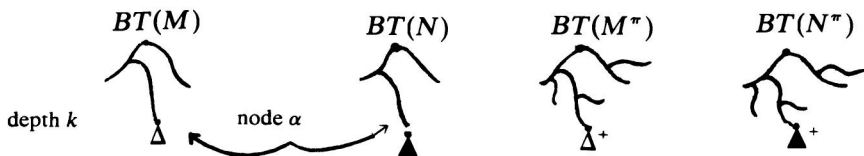
and the internal nodes with free head variable x_i

$$(*) \quad \lambda y_1 \cdots y_s. x_i \quad \text{by} \quad \lambda y_1 \cdots y_s w_{t+1} \cdots w_{q+1}. w_{q+1} \begin{array}{c} \swarrow \quad \downarrow \quad \searrow \\ x_i \square_1 \cdots \square_t w_{t+1} \cdots w_q \end{array}$$

(here $q > t$ is used). Clearly $\text{BT}(M^\pi)$ and $\text{BT}(N^\pi)$ are head original up to k .

Claim: These trees separate at depth k .

Since $\text{BT}(M) \equiv_k \text{BT}(N)$, also $\text{BT}(M^\pi) \equiv_k \text{BT}(N^\pi)$. By assumption $\text{BT}(M)$, $\text{BT}(N)$ are not mergeable at some node α with $d(\alpha) = k$. Consider the Böhm trees



Suppose Δ and $\blacktriangle$ have both the free head variable x_i . Referring to $(*)$, Δ^+ and $\blacktriangle^+$ are top mergeable iff $s + (q + 1 - t) - (1 + q) = s' + (q' + 1 - t') - (1 + q')$ iff $s - t = s' - t'$ which is not the case since Δ and $\blacktriangle$ are not top mergeable. Hence $\text{BT}(M^\pi)$, $\text{BT}(N^\pi)$ are not mergeable at α , i.e. separate at depth k . The same conclusion holds in the other cases (x_i is head variable of Δ , not of $\blacktriangle$ ($q > s$ $s' + t$ insures that Δ^+ and $\blacktriangle^+$ have different head variables and hence are not top mergeable); x_i is not head variable of either Δ or $\blacktriangle$). $\square$

6.16. COROLLARY. *If $\text{BT}(M)$, $\text{BT}(N)$ separate at depth $k > 0$, then for some π , $\text{BT}(M^\pi)$, $\text{BT}(N^\pi)$ separate at depth $k - 1$.*

PROOF. By 6.14 and 6.15. $\square$

6.17. LEMMA. *If $\text{BT}(M), \text{BT}(N)$ separate at level 0, then for some π , M^π is solvable, N^π is unsolvable, or conversely.*

PROOF. If M is unsolvable, $\text{BT}(M) = \Omega$ and hence N is solvable since $\text{BT}(M), \text{BT}(N)$ differ at level 0. In this case take π the identity. If M, N are solvable, say $M \rightarrow \lambda x_1 \cdots x_n. x_i M_1 \cdots M_m$, $N \rightarrow \lambda x_1 \cdots x_{n'}. x_{i'} N_1 \cdots N_{m'}$, then by assumption $i \neq i'$ or $n - m \neq n' - m'$. In case $i \neq i'$ take $P^\pi = P[x_i/(\lambda y_1 \cdots y_m. I)x_i][x_{i'}/\Omega x_{i'}]$. Then $M^\pi = I$ and $N^\pi = \lambda x_1 \cdots x_{n'}. \Omega \cdots = \Omega \pmod{\mathcal{H}}$ and hence unsolvable. In case $i = i'$ and $n - m \neq n' - m'$, let $P^{\pi_0} = P x_1 \cdots x_p \Omega$ with p large enough ($\geq \max(m, n, m', n')$). Then $M^{\pi_0} = x_i M_1 \cdots M_m x_{n+1} \cdots x_p \Omega$. $N^{\pi_0} = x_i N_1 \cdots N_{m'} x_{n'+1} \cdots x_p \Omega$. The length of the sequences after x_i is $m + p - n + 1$, $m' + p - n' + 1$ respectively which differ since $n - m \neq n' - m'$. Hence by defining $\pi = \pi_1 \circ \pi_0$, with $P^{\pi_1} = P[x_i/U^q x_i]$ where $U^q = \lambda y_1 \cdots y_n. y_j$ is an appropriate selector, the required π is found. $\square$

PROOF OF THEOREM 6.8. Suppose $M = N \in \mathcal{H}^*$, but $\text{BT}(M) \not\sim_\eta \text{BT}(N)$. By 6.11 for some M', N' , $\lambda \eta \vdash M = M', N = N'$ and $\text{BT}(M'), \text{BT}(N')$ separate at depth k . By iterated application of 6.16, $\text{BT}(M'^{\pi_0}), \text{BT}(N'^{\pi_0})$ separate at depth 0 for some π_0 . Hence it follows from 6.17 that for some π_1 , M'^{π_1} is, say, solvable and N'^{π_1} is unsolvable. Now for each π there is a $C_\pi[\cdot]$ such that $\pi(P) = C_\pi[P]$ (a substitution $M[x/Nx]$ can be written as $C[M]$ with $C[\cdot] = (\lambda x. [\cdot])(Nx)$). So $C_{\pi_1}[M']$ is solvable and $C_{\pi_1}[N']$ is unsolvable, hence $\mathcal{H}^* \not\vdash M' = N'$ by the proof of 5.6. But this contradicts $\mathcal{H}^* \vdash M = N$, since $\mathcal{H}^*$ proves extensionality (see 5.9(ii)). $\square$

7. Analysis of D_∞

Using Böhm trees it is possible to give an elegant characterization of equality of terms in $\mathcal{P}\omega$ and D_∞ .

7.1. THEOREM. (i) $D_\infty \models M = N \Leftrightarrow \mathcal{H}^* \vdash M = N \Leftrightarrow \text{BT}(M) \sim_\eta \text{BT}(N)$.
(ii) $\mathcal{P}\omega \models M = N \Leftrightarrow \text{BT}(M) = \text{BT}(N)$.

The first result is due to Hyland and Wadsworth, the second to Hyland. We will only present the proof of (i) (see 7.16). See HYLAND [1976] or BARENDREGT [to appear] for the other proof.

7.2. COROLLARY (see 6.6 and 6.7 for a definition of the terms involved). *The equalities $Ax = Ay$, $Y_z = Y$, $J = I$ hold in D_∞ but cannot be proved algebraically, i.e. by conversion.*

PROOF. The equality in D_∞ follows by 6.6, 6.7 and the theorem. By the Church–Rosser theorem the equalities are not provable in λ . $\square$

7.3. DEFINITION. (In the sequel $[\![\cdot]\!]$ is $[\![\cdot]\!]^{P_\infty}$.) The $\lambda\Omega$ -calculus was introduced by Wadsworth as a tool for examining D_∞ . $\lambda\Omega$ -terms are defined by adding to the formation rules of terms (see 1.7): Ω is a term. The interpretation in D_∞ is extended to $\lambda\Omega$ -terms by setting $[\![\Omega]\!]_p = \perp$. Reduction for $\lambda\Omega$ -terms is ordinary reduction extended with the axioms $\lambda x\Omega \rightarrow \Omega$ and $\Omega P \rightarrow \Omega$. A $\lambda\Omega$ -term P has an Ω nf Q iff $P \rightarrow Q$ is an Ω reduction and Q has no subterm $(\lambda x.R)S$, $\lambda x\Omega$ or ΩR . Note that Ω reduction preserves the value in D_∞ since $\perp d = \perp$, hence also $\lambda x.\perp = \perp$. If P has a nf in the original sense, then P has an Ω nf, since replacements $\lambda x\Omega \rightarrow \Omega$ or $\Omega R \rightarrow \Omega$ decrease the length of a term. Böhm trees of $\lambda\Omega$ -terms are defined by letting $\text{BT}(\Omega) = \Omega$.

7.4. DEFINITION. Approximation.

(i) Let P, Q be $\lambda\Omega$ -terms. P approximates Q , notation $P \sqsubseteq Q$, iff $\text{BT}(P)$ results from $\text{BT}(Q)$ by replacing some subtrees by the tree Ω (e.g. $\lambda x.x\Omega \sqsubseteq \lambda x.IxK$).

(ii) Let M be a λ -term. P is an approximate normal form (anf) of M iff $P \sqsubseteq M$ and P is an Ω nf.

(iii) $A(M) = \{P \mid P \text{ is an anf of } M\}$.

(iv) M^k is the anf of M such that $\text{BT}(M^k)$ results from $\text{BT}(M)$ by replacing all labels at nodes of depth k by Ω and cancelling the deeper nodes. Note that $M^k \in A(M)$.

7.5. EXAMPLE. $\lambda f.f(\Omega) \sqsubseteq \lambda f.f((\lambda x.f(xx))(\lambda x.f(xx)))$ hence $\lambda f.f(\Omega)$ is an anf of the fixed point combinator Y (defined after 2.1). In fact

$$Y^k = \lambda f.f^k(\Omega), \quad A(Y) = \{\Omega \leftarrow \lambda f.\Omega, \lambda f.f\Omega, \lambda f.f(f\Omega), \dots\}.$$

7.6. LEMMA. $P \sqsubseteq Q \Rightarrow [\![P]\!] \sqsubseteq [\![Q]\!]$.

PROOF. P is Q with some subterms replaced by Ω . Now $[\![\Omega]\!] = \perp$, the least element of D_∞ . The result follows since application and abstraction in D_∞ are monotonic (by their continuity). $\square$

The following theorem is quite useful for determining the value of λ -terms in D_∞ . The proof will be given in 7.18–7.24.

7.7. APPROXIMATION THEOREM (conjectured by Scott, proved by Hyland, and improved by Wadsworth) *For λ -terms M :*

$$\llbracket M \rrbracket = \bigsqcup \{ \llbracket P \rrbracket \mid P \in A(M) \}.$$

The same theorem holds in $\mathcal{P}\omega$ with the $\bigsqcup$ replaced by $\bigcup$.

7.8. COROLLARY. $\llbracket M \rrbracket = \bigsqcup_k \llbracket M^k \rrbracket$.

PROOF. Let $P \in A(M)$, then $P \sqsubset M$, P Ω -nf. Now let all nodes in $\text{BT}(P)$ have depth $< k$. Then $\llbracket P \rrbracket \sqsubseteq \llbracket M^k \rrbracket$ and the result follows. $\square$

7.9. THEOREM. *The following are equivalent for $M \in \Lambda$:*

- (i) M is solvable,
- (ii) $\llbracket M \rrbracket \neq \perp$,
- (iii) M has a hnf.

PROOF. It may be assumed that M is closed (if not, consider $\lambda \vec{x}. M$ and note $\lambda d. \perp = \perp$).

(i) $\Rightarrow$ (ii) Let M be solvable. Then for some $\vec{N}$, $\lambda \vdash M\vec{N} = I$. If $\llbracket M \rrbracket = \perp$, then $\llbracket I \rrbracket = \llbracket M\vec{N} \rrbracket = \perp \llbracket \vec{N} \rrbracket = \perp$, contradicting $\perp d = \perp$. So $\llbracket M \rrbracket \neq \perp$.

(ii) $\Rightarrow$ (iii) Suppose M has no hnf. Then $A(M) = \{\Omega\}$, hence by 7.7, $\llbracket M \rrbracket = \perp$.

(iii) $\Rightarrow$ (i) Suppose $M \rightarrow \lambda \vec{x}. x_i M_1 \cdots M_m$. Then by giving M enough arguments $N \equiv \lambda a_1 \cdots a_m. I$, M can be solved. $\square$

7.10. COROLLARY. D_∞ is sensible; hence $\lambda\eta + \mathcal{K}$ is consistent.

PROOF. By 7.9, M is unsolvable $\Rightarrow \llbracket M \rrbracket = \perp$; so $D_\infty \models \mathcal{K}$. Hence by 4.23, $D_\infty \models \lambda\eta + \mathcal{K}$. $\square$

Another consequence of the approximation theorem is a connection between the fixed point combinator and the least fixed point operator for complete lattices.

7.11. THEOREM (Tarski). *Let D be a complete lattice. Each continuous*

$f : d \rightarrow D$ has a fixed point. Moreover there is a $Y^* \in [[D \rightarrow D] \rightarrow D]$ such that Y^*f is the minimal fixed point of f .

PROOF. Let $Y^*f = \bigsqcup \{f^n(\perp) \mid n \in \omega\}$. Then Y^* is continuous by 4.8 and 4.5. Since $\perp \sqsubseteq f(\perp)$, so $f^n(\perp) \sqsubseteq f^{n+1}(\perp)$ $\{f^n(\perp) \mid n \in \omega\}$ is directed, hence Y^*f is a fixed point of f . If $f(x) = x$, then since $\perp \sqsubseteq x$, $f(\perp) \sqsubseteq f(x) \sqsubseteq x$, etc., so $Y^*f \sqsubseteq x$. $\square$

Let Y_{Tarski} be the element of D_∞ corresponding to the fixed point operator Y^* and let $Y_{\text{Curry}} = \llbracket Y \rrbracket$, with Y defined after 2.1.

7.12. THEOREM (Park). *In Scott's model D_∞ , $Y_{\text{Tarski}} = Y_{\text{Curry}}$.*

PROOF. By 7.8 and 7.5,

$$Y_{\text{Curry}}d = (\bigsqcup_k \llbracket \lambda f. f^k(\Omega) \rrbracket)d = \bigsqcup_k d^k(\perp) = Y_{\text{Tarski}}d$$

by definition. The result now follows by extensionality. $\square$

Results analogous to 7.11 and 7.12 hold for $\mathcal{P}\omega$.

In order to prove the characterization of equality in D_∞ , the following definition is needed.

- 7.13. DEFINITION.** (i) $M \sqsubseteq_k N$ iff $M^k \sqsubseteq N^k$;
(ii) $M <_k N$ iff $\exists M', N' [\lambda\eta \vdash M = M', \lambda\eta \vdash N = N' \text{ and } M' \sqsubseteq_k N']$;
(iii) $M < N$ iff $\forall k M <_k N$.

Note that if $\text{BT}(M) \sim_\eta \text{BT}(N)$, then $M < N$ and $N < M$. The converse follows from 7.14 and 7.16. Also note $M^k < M$. $<$ is transitive, since if $M_1^k \sqsubseteq N_1^k$ and $N_2^k \sqsubseteq L_2^k$, where $\lambda\eta \vdash N_1 = N_2$, then by some $\beta\eta$ -conversion M_1 becomes M_2 such that $M_2^k \sqsubseteq N_2^k \sqsubseteq L_2^k$.

7.14. THEOREM. $M < N \Rightarrow \llbracket M \rrbracket \sqsubseteq \llbracket N \rrbracket$.

The proof is given in 7.25–7.27.

7.15. COROLLARY. $\text{BT}(M) \sim_\eta \text{BT}(N) \Rightarrow \llbracket M \rrbracket = \llbracket N \rrbracket$.

PROOF. By the remark following 7.13. $\square$

7.16. THEOREM (Hyland; Wadsworth). *The following are equivalent for $M, N \in \Lambda$.*

- (i) $\text{BT}(M) \sim_\eta \text{BT}(N)$,
- (ii) $D_\infty \models M = N$,
- (iii) $\mathcal{H}^* \vdash M = N$.

PROOF. (i) $\Rightarrow$ (ii) is 7.15.

(ii) $\Rightarrow$ (iii) by 5.9 since $D_\infty \models \mathcal{H}$ (7.10).

(iii) $\Rightarrow$ (i) is 6.8. $\square$

Note that $\text{Th}(D_\infty) \subset \mathcal{H}^* \Rightarrow \text{Th}(D_\infty) = \mathcal{H}^*$ is not obvious (as would have been the case in ordinary model theory): since the language of the λ -calculus does not contain logical operators, $\text{Th}(\mathcal{M})$ is not necessarily a complete set of sentences.

7.17. COROLLARY. (i) $\text{Th}(D_\infty) = \mathcal{H}^*$; hence for every D , D_∞ satisfies the same set of equations,

(ii) D_∞^0 is algebraically simple.

PROOF. (i) Immediate.

(ii) $D_\infty^0 = \mathcal{M}^0(\text{Th}(D_\infty^0)) = \mathcal{M}^0(\mathcal{H}^*)$ hence the result follows from 5.11. $\square$

In order to prove the approximation theorem the following indexed $\lambda\Omega$ -calculus was introduced by Hyland and Wadsworth.

7.18. DEFINITION. The set of *indexed* ($\lambda\Omega$)-terms is defined by adding to the formation rules of the $\lambda\Omega$ -terms: if M is an indexed $\lambda\Omega$ -term, so is $(M)^p$ for all $p \in \omega$. The interpretation of $\lambda\Omega$ -terms in D_∞ is extended to indexed terms by adding the clause $\llbracket (M)^p \rrbracket_p = (\llbracket M \rrbracket_p)_p$. Thus the superscripts p are considered as the projections $\Phi_{\infty, p} : D_\infty \rightarrow D_p$.

If M is an indexed term, M^* is obtained from M by leaving out all superscripts. Note that $\llbracket M \rrbracket \sqsubseteq \llbracket M^* \rrbracket$. A *completely* indexed term M is such that each subterm occurrence N of M^* has an index in M (i.e. occurs as part of $(N)^p$ in M).

7.19. DEFINITION. The reduction relation on $\lambda\Omega$ -terms is extended to indexed $\lambda\Omega$ -terms by adding the axioms

$$\lambda x. \Omega^p \rightarrow \Omega^0; \quad \Omega^p M \rightarrow \Omega^0; \quad (\lambda x. M)^{p+1} N \rightarrow (M[x/N^p])^p;$$

$$(\lambda x. M)^0 N \rightarrow (M[x/\Omega^0])^0; \quad (M^p)^q \rightarrow M^{\min(p, q)}$$

and the rule $M \rightarrow N \Rightarrow M^p \rightarrow N^p$. An indexed term M has a *nf* if for some N , $M \rightarrow N$ and N^* is in Ω nf.

7.20. LEMMA. *Let M, N be indexed terms, and $M \rightarrow N$ as indexed terms. Then*

- (i) $N^* \sqsubset M^*$.
- (ii) $\llbracket M \rrbracket = \llbracket N \rrbracket$.

PROOF. (i) The approximation comes in at reductions like $(\lambda x. x)^0 N \rightarrow \Omega^0$.

(ii) By 4.19 and 4.15(i), (v). $\square$

7.21. DEFINITION. (i) An *indexing* I on M is a mapping that assigns to each subterm occurrence of M an index. M^I is the resulting completely indexed term.

(ii) $\tau(M) = \{M^I \mid I \text{ indexing on } M\}$.

7.22. LEMMA. *Let M be a λ -term. Then $\llbracket M \rrbracket = \sqcup \{\llbracket N \rrbracket \mid N \in \tau(M)\}$.*

PROOF. By induction on the structure of M , using 4.15(iii). $\square$

7.23. LEMMA. *Each completely indexed term has a nf.*

PROOF. M has a p -redex iff $(\lambda x. P)^p Q$ occurs in M . The *order* of M is the maximal p such that M has a p -redex. By induction on the order p of M , it is shown that M has a nf.

$p = 0$: contractions like $(\lambda x. P)^0 Q \rightarrow (P[x/\Omega^0])^0$, $\lambda x. \Omega^p \rightarrow \Omega^0$, $\Omega^p M \rightarrow \Omega^0$ and $(M^p)^q \rightarrow M^{\min(p, q)}$ decrease the length of a term, hence each term of order 0 has a nf.

$p = n + 1$: replacing the rightmost $n + 1$ redex $(\lambda x. P)^{n+1} Q$ by $(P[x/Q^n])^n$ and then replacing terms $(Q^n)^q$ by $Q^{\min(n, q)}$ results in a term with one less occurrence of a p -redex. (Prime example (some indices are omitted):

$$\begin{aligned} & (\lambda ab. baa)^{n+1}((\lambda x. x^{n+1} R)^{n+1}(\lambda z. z)^{n+2}) \rightarrow (\lambda ab. baa)^{n+1}, \\ & \rightarrow (\lambda ab. baa)^{n+1}(((\lambda z. z)^n)^{n+1} R) \rightarrow (\lambda ab. baa)^{n+1}((\lambda z. z)^n R). \end{aligned}$$

After a finite number of steps the term is reduced to one with order n and the induction hypothesis applies. $\square$

7.24. PROOF OF 7.7. $\llbracket M \rrbracket = \sqcup \{\llbracket N \rrbracket \mid N \in \tau(M)\} = \sqcup \{\llbracket L \rrbracket \mid \exists N \in \tau(M) L \text{ nf of } N\} \subseteq \sqcup \{\llbracket L^* \rrbracket \mid \exists N \in \tau(M) L \text{ nf of } N\} \subseteq \sqcup \{\llbracket N \rrbracket \mid N \in A(M)\} \subseteq \llbracket M \rrbracket$.

The five (in)equalities follow respectively from 7.22, 7.20(ii) and 7.23, $\llbracket L \rrbracket \subseteq \llbracket L^* \rrbracket$, $L^* \in A(M)$ since by 7.20(i) $L^* \sqsubset N^* = M$, and from $N \in A(M) \Rightarrow \llbracket N \rrbracket \subseteq \llbracket M \rrbracket$ (by 7.6). $\square$

Now Hyland's proof of 7.14 will be presented.

7.25. LEMMA. *Let $P \neq \Omega$ be an Ω nf and $P < Q$. Then $\text{BT}(P)$, $\text{BT}(Q)$ are top mergeable, $\lambda\eta \vdash P = \lambda x_1 \cdots x_n. x_i P_1 \cdots P_m$ and $\lambda\eta \vdash Q = \lambda x_1 \cdots x_n. x_i Q_1 \cdots Q_m$ say, and $P_1 < Q_1, \dots, P_m < Q_m$; the $P_1, \dots, P_m$ are in Ω nf.*

PROOF. Only η -reductions affect the Böhm trees. Therefore, since $P < Q$, after some η -changes the tops of $\text{BT}(P)$, $\text{BT}(Q)$ are the same, i.e. they are top mergeable. The P_i 's are either already part of P or a variable created by an η -expansion; therefore they are in Ω nf. Since $P <_{k+1} Q$, it follows that $P_i <_k Q_i$ for all k ; hence $P_i < Q_i$. $\square$

7.26. LEMMA. *Let P be an Ω nf. Then $P < N \Rightarrow \llbracket P \rrbracket \subseteq \llbracket N \rrbracket$.*

PROOF. By induction on the structure of P ,

Case 1. $P \equiv \Omega$. Then we are done.

Case 2. $P \equiv x$. Then, using $x <_1 N$, $\lambda \vdash N = \lambda y_1 \cdots y_n. x N_1 \cdots N_n$. By 7.22 it is sufficient to show that for any indexing I of x $\llbracket x \rrbracket^I \subseteq \llbracket N \rrbracket$. This is done by induction on $k = I(x)$.

If $k = 0$, then $\llbracket (x)^0 \rrbracket = \llbracket \lambda y_1 \cdots y_n. (x)^0 \Omega \cdots \Omega \rrbracket \subseteq \llbracket N \rrbracket$ since in D_x $x_0 = x_0 \cdot \perp = \lambda y. x_0$ by 4.19(ii).

If $I(x) = k + 1$, then $\llbracket (x)^{k+1} \rrbracket = \llbracket \lambda y_1 \cdots y_n. (x)^{k+1} (y_1)^k \cdots (y_n)^{k+1-n} \rrbracket$ by 4.19(i) (and 4.14(ii)). Since $x < N$, for all i , $1 \leq i \leq n$, $y_i < N_i$, hence by the induction hypothesis $\llbracket y_i^{k+1-i} \rrbracket \subseteq \llbracket N_i \rrbracket$. So we have $\llbracket (x)^{k+1} \rrbracket \subseteq \llbracket N \rrbracket$.

Case 3. $P \equiv \lambda x_1 \cdots x_m. x P_1 \cdots P_n$, $P_1, \dots, P_n$ Ω nf's. Then since $P < N$ for some P', N' with $\lambda\eta \vdash P' = P$, $\lambda\eta \vdash N' = N$ one has $P' \equiv \lambda x_1 \cdots x_p. x P'_1 \cdots P'_q$, $N' \equiv \lambda x_1 \cdots x_p. x N'_1 \cdots N'_q$ and $P'_1 < N'_1, \dots, P'_q < N'_q$.

By the induction hypothesis $\llbracket P_i \rrbracket \subseteq \llbracket N \rrbracket, \dots$ hence $\llbracket P \rrbracket = \llbracket P' \rrbracket \subseteq \llbracket N' \rrbracket = \llbracket N \rrbracket$. $\square$

7.27. PROOF OF THEOREM 7.14. Suppose $M < N$. Then $\forall k$ $M^k < N$, hence by 7.26, $\forall k$ $\llbracket M^k \rrbracket \subseteq \llbracket N \rrbracket$. Therefore $\llbracket M \rrbracket = \bigsqcup \llbracket M^k \rrbracket \subseteq \llbracket N \rrbracket$. $\square$

References

BARENDREGT, H.P.

[1975] Normed uniformly reflexive structures, in: *λ -Calculus and Computer Science*, edited by C. Böhm, Lecture Notes in Computer Science, Vol. 37 (Springer, Berlin) pp. 272–286.

- [1977] *The Lambda Calculus, its Syntax and Semantics* (North-Holland, Amsterdam) to appear.
- BÖHM, C.
 [1968] Alcune proprietà della forma β - η -normali del λ -K-calcolo, *Pubbl. IAC-CNR n. 696*, Roma.
- BRUIJN, N.G. DE
 [1972] Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem, *Indag. Math.*, **34** (5), 381-392.
- CHURCH, C.
 [1941] *The Calculi of Lambda-Conversion* (Princeton University Press, Princeton, RI).
- CURRY, H.B. and R. FEYS
 [1958] *Combinatory Logic*, Vol. I (North-Holland, Amsterdam).
- CURRY, H.B., R. HINDLEY and J. SELDIN
 [1972] *Combinatory Logic*, Vol. II (North-Holland, Amsterdam).
- HINDLEY, R., B. LERCHER and J. SELDIN
 [1972] *Introduction to Combinatory Logic* (Cambridge University Press, Cambridge).
- HYLAND, J.M.E.
 [1976] A syntactic characterization of the equality in some models of the λ -calculus, *J. London Math. Soc.*, **12** (2), 361-370.
- MANN, C.R.
 [1975] The connection between equivalence of proofs and cartesian closed categories, *Proc. London Math. Soc.*, **31** (3), 289-310.
- NAKAJIMA, R.
 [1975] Infinite normal forms for λ -calculus, in: *λ -Calculus and Computer Science*, edited by C. Böhm, *Lecture Notes in Computer Science*, Vol. 37 (Springer, Berlin) pp. 62-82.
- PLOTKIN, G.
 [1972] A set-theoretical definition of application, School of A.I., Memo MIP-R-95, Edinburgh.
 [1974] The λ -calculus is ω -incomplete, *J. Symbolic Logic*, **39** (2), 313-317.
- SCOTT, D.
 [1972] Continuous lattices, in: *Toposes, Algebraic Geometry and Logic*, edited by F.W. Lawvere, *Lecture Notes in Mathematics*, Vol. 274 (Springer, Berlin) pp. 97-136.
 [1975a] Lambda calculus and recursion theory, in: *Proceedings of the Third Scandinavian Logic Symposium*, edited by S. Kanger (North-Holland, Amsterdam) pp. 154-193.
 [1975b] Combinators and classes, in: *λ -Calculus and Computer Science*, edited by C. Böhm, *Lecture Notes in Computer Science*, Vol. 37 (Springer, Berlin) pp. 1-26.
 [1975c] Some philosophical issues concerning theories of combinators, in: *λ -Calculus and Computer Science*, edited by C. Böhm, *Lecture Notes in Computer Science*, Vol. 37 (Springer, Berlin) pp. 346-366.
 [1976] Data types as lattices, *SIAM J. Comput.*, **5** (3), 522-587.
- TROELSTRA, A.S., editor
 [1973] *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*, *Lecture Notes in Mathematics*, Vol. 344 (Springer, Berlin).
- WADSWORTH, C.P.
 [1976] The relation between lambda-expressions and their denotations, *SIAM J. Comput.*, **5** (3), 488-521.

*A Mathematical Incompleteness in Peano Arithmetic**

JEFF PARIS
LEO HARRINGTON

Contents

1. An extension of the Finite Ramsey Theorem.	1134
2. Proofs of 1.2 and 1.3	1135
3. Refinements	1141
References	1142

* *Editor's Note:* Since 1931, the year Godel's Incompleteness Theorems were published, mathematicians have been looking for a strictly mathematical example of an incompleteness in first-order Peano arithmetic, one which is mathematically simple and interesting and does not require the numerical coding of notions from logic. The first such examples were found early in 1977, when this *Handbook* was almost finished. We are pleased to be able to include a final chapter which presents the most striking example to date. It is a fitting conclusion since it brings together ideas from all Parts of the *Handbook*.

1. An extension of the Finite Ramsey Theorem

In this chapter we present a recent discovery in mathematical logic. We investigate a reasonably natural theorem of finitary combinatorics, a simple extension of the Finite Ramsey Theorem. This chapter is mainly devoted to demonstrating that this theorem, while true, is not provable in Peano arithmetic.

The first examples of strictly mathematical statements about natural numbers which are true but not provable in PA (Peano arithmetic) were due to the first author (see PARIS [to appear]) and grew out of the work in PARIS and KIRBY [to appear]. The second author's contribution was to show that Paris's proof could be carried through with the particularly simple extension of the Finite Ramsey Theorem mentioned above (and stated precisely in 1.2).

Since we are going to work extensively with the partition calculus, the reader would be wise to consult pages 390–393 of Chapter B.3 for basic information and pages 393–395 for a proof of the Infinite Ramsey Theorem.

1.1. DEFINITION. We call a finite set H of natural numbers *relatively large* if $\text{card}(H) \geq \min(H)$. Given natural numbers e, r, k and M , we use the notation

$$M \xrightarrow{*} (k)^e_r$$

to mean that for every partition $P : [M]^e \rightarrow r$ there is a relatively large $H \subseteq M$ which is homogeneous for P and of cardinality at least k .

1.2. THEOREM. *For all natural numbers e, r and k there is an M such that $M \xrightarrow{*} (k)^e_r$.*

Without the $*$ under the arrow which makes the homogeneous sets relatively large, this would just be the Finite Ramsey Theorem. The Finite Ramsey Theorem is provable in Peano Arithmetic. Our proof of 1.2 will use the Infinite Ramsey Theorem, and cannot be carried out in PA.

1.3. MAIN THEOREM. *The combinatorial principle of 1.2 is not provable in Peano Arithmetic.*

For the reader who is not used to working in PA, and so does not even see how to formulate 1.2 in PA, we would remark that PA is equivalent

(for statements about natural numbers) to the result of replacing the axiom of infinity by its negation in the usual axioms ZF of set theory (see Chapter B.1), and 1.2 can be formulated in this theory directly, without any coding.

2. Proofs of 1.2 and 1.3

We first prove 1.2. Fix e, r and k , and suppose there were no M of the desired kind. Call P a counterexample for M if P is a partition of $[M]^e$ into r pieces with no relatively large homogeneous set of size at least k . We may view the set of counterexamples as a finitely branching infinite tree. That is, if P and P' are counterexamples for M and M' respectively, we put P below P' in our tree just in case $M < M'$ and P is the restriction of P' to $[M]^e$. By König's Lemma there is a $P : [\omega]^e \rightarrow r$ such that for every M , the restriction of P to $[M]^e$ is a counterexample for M . By the Infinite Ramsey Theorem, there is an infinite $H \subseteq \omega$ homogeneous for P . But then by choosing M large enough (compared to k and $\min(H)$) we see that $H \cap M$ is, after all, a relatively large homogeneous set for $P \upharpoonright [M]^e$ of size at least k . $\square$

Looking ahead to Section 3, we point out that, for each e , the above proof can be formalized in PA. (The proof on pages 393–395 of $\omega \rightarrow (\omega)^e$ is naturally formalized, by induction on e , in restricted- $(\Pi^0_\infty - \text{CA})$, which is conservative over PA (see page 940).) Thus, for every e ,

$$\text{PA} \vdash \forall r, k \exists M (M \xrightarrow{*} (k)^e).$$

We now begin the proof of 1.3, which will take up the remainder of this section. We define a certain theory T in 2.1 and then show $\text{Con}(T) \rightarrow \text{Con}(\text{PA})$ is provable in PA. The proof will be concluded by showing, in PA, that the combinatorial principle of 1.2 implies $\text{Con}(T)$.

For the purpose of the following we identify finite subsets of ω with finite increasing sequences from ω . The theory T is expressed in the language of PA plus infinitely many new constant symbols $c_0, c_1, \dots$.

2.1. DEFINITION. The axioms of T are as follows:

- (i) The usual recursive defining equations for $+$, $\times$, $<$, plus the induction axioms but only for limited formulas.
- (ii) For each $i = 0, 1, \dots$, the axiom $(c_i)^2 < c_{i+1}$.
- (iii) For each finite subset $i = i_1, \dots, i_r$ of ω , let $c(i) = c_{i_1}, \dots, c_{i_r}$.

For each $i < \mathbf{k}, \mathbf{k}'$ and each limited formula $\psi(\mathbf{y}; \mathbf{z})$ (where $\mathbf{k}, \mathbf{k}'$ and $\mathbf{z}$ all have the same length) we have the axiom:

$$\forall \mathbf{y} < c_i [\psi(\mathbf{y}; c(\mathbf{k})) \leftrightarrow \psi(\mathbf{y}; c(\mathbf{k}'))].$$

2.2. PROPOSITION. $\text{Con}(T)$ implies $\text{Con}(\text{PA})$.

PROOF. Let $\mathfrak{A} \models T$ and let I be the initial segment of $\mathfrak{A}$ of those $a < c_i$ for some $i \in \omega$. By (ii), I is closed under $+$ and $\times$. It will be enough to show the following.

2.3. CLAIM. $\mathfrak{S} = \langle I, +, \times, < \rangle$ is a model of PA.

For each formula $\theta(\mathbf{y})$ from the language of PA, define a limited formula $\theta^*(\mathbf{y}; \mathbf{z})$ as follows. Write θ in prenex normal form, say $\exists x_1 \cdots \forall x_r \varphi(\mathbf{x}; \mathbf{y})$ where φ is quantifier free. Then $\theta^*(\mathbf{y}; z_1, \dots, z_r)$ is $\exists x_1 < z_1 \cdots \forall x_r < z_r \varphi(\mathbf{x}; \mathbf{y})$.

2.4. CLAIM. Given $i < \mathbf{k}, a < c_i$, and $\theta(\mathbf{y})$, where $\mathbf{k}, a$ and $\mathbf{y}$ are all of the appropriate length,

$$\mathfrak{S} \models \theta(a) \text{ if and only if } \mathfrak{A} \models \theta^*(a; c(\mathbf{k})).$$

Notice that 2.3 is an immediate consequence of 2.4 since part (i) of 2.1 guarantees that for all θ , $\mathfrak{A}$ will satisfy induction for θ^* . Then proof of 2.4 proceeds by induction on θ . Suppose $\theta(\mathbf{y})$ is $\exists x \psi(x, \mathbf{y})$. Thus $\theta^*(\mathbf{y}; \mathbf{z})$ is $\exists x < z_1 \psi^*(x, \mathbf{y}; z_2, \dots, z_r)$. So $\mathfrak{S} \models \theta(a)$ iff for some b in I and some j (where $\min(j)$ is large) $\mathfrak{A} \models \psi^*(b, a; c(j))$, which happens iff for some $\mathbf{k}'$ (again, where $\min(\mathbf{k}')$ is large) $\mathfrak{A} \models \theta^*(a; c(\mathbf{k}'))$ which, by 2.1(iii), is the case iff $\mathfrak{A} \models \theta^*(a; c(\mathbf{k}))$. $\square$

The attentive reader should observe that the proof of 2.2 can be formalized in PA (in a way similar to Section 6 of Chapter D.1). Also, one should notice that for the purposes of the above proof, we can weaken 2.1(iii) to those limited formulas $\psi(\mathbf{y}; \mathbf{z})$ of the form $\theta^*(\mathbf{y}; \mathbf{z})$ for some $\theta(\mathbf{y})$

2.5. PROPOSITION. *The combinatorial principal of 1.2 implies $\text{Con}(T)$.*

By Gödel's Second Incompleteness Theorem (see page 825), 2.5 and 2.2 yield our main theorem, provided of course that 2.5, like 2.2, is proved in PA.

Before beginning the proof of 2.5, we point out a few facts about partitions.

2.6. LEMMA. *Given partitions P_0 and P_1 of $[M]^e$ into r_0 and r_1 pieces, there is a partition P of $[M]^e$ into $r_0 \cdot r_1$ pieces such that for $H \subseteq M$, H is homogeneous for P iff H is homogeneous for both P_0 and P_1 .*

PROOF. Let $P(a) = \langle P_0(a), P_1(a) \rangle$. $\square$

2.7. LEMMA. *A set $H \subseteq M$ is homogeneous for a partition P of $[M]^e$ iff every subset of H of size $e + 1$ is homogeneous for P .*

PROOF. Let $a = a_1, \dots, a_e$ be the first e elements of H . Pick $b = b_1, \dots, b_e$ so that $P(a) \neq P(b)$ and so that $b_1 + \dots + b_e$ is minimized. If i is the least index such that $a_i \neq b_i$, then $\{a_1, \dots, a_i, b_i, \dots, b_e\}$ is not homogeneous and of size $e + 1$. $\square$

We define $\sqrt{r}$ to be the first natural number s such that $s^2 \geq r$. Notice that for most r (i.e., for $r \geq 7$), $r \geq 1 + 2\sqrt{r}$.

2.8. LEMMA. *Given $P : [M]^e \rightarrow r$ there is a $P' : [M]^{e+1} \rightarrow (1 + 2\sqrt{r})$ such that for all $H \subseteq M$ of cardinality $> e + 1$, H is homogeneous for P iff H is homogeneous for P' .*

PROOF. Let $s = \sqrt{r}$. Define functions Q (for quotient) and R (for remainder) both mapping $[M]^e$ into s by the equation $P(a) = s \cdot Q(a) + R(a)$. For $b = b_1, \dots, b_e, b_{e+1}$ in $[M]^{e+1}$, let $b' = b_1, \dots, b_e$. We now define our desired P' on $[M]^{e+1}$ by:

$$P'(b) = \begin{cases} 0 & \text{if } b \text{ is homogeneous for } P, \\ \langle 0, R(b') \rangle & \text{if } b \text{ is homogeneous for } Q \text{ but not for } P, \\ \langle 1, Q(b') \rangle & \text{otherwise,} \end{cases}$$

Let H be homogeneous for P' of cardinality $> e + 1$, and let c be the first $e + 1$ members of H . We need to see that $P'(c) = 0$ to verify that H is homogeneous for P , by 2.7. Note that for each a in $[c]^e$ there is a b in $[H]^{e+1}$ such that $b' = a$. Suppose $P'(c) = \langle 1, i \rangle$. Then, by the previous remark, $Q(a) = i$ for all a in $[c]^e$ so that c is homogeneous for Q , contradicting the definition of P' . So suppose $P'(c) = \langle 0, j \rangle$ so that c is Q homogeneous, say $Q(a) = i$ for all a in $[c]^e$. But then $P(a) = s \cdot i + j$ for all

such a so that c is homogeneous for P , again contradicting the definition of P' . $\square$

2.9. LEMMA. *Suppose we are given n partitions $P_i : [M]^{e_i} \rightarrow r_i$, all $i < n$. Let $e = \max_i e_i$ and $r = \prod_i \max(r_i, 7)$. There is a partition $P : [M]^e \rightarrow r$ such that for all $H \subseteq M$ of cardinality $> e$, H is homogeneous for P iff H is homogeneous for all the P_i .*

PROOF. Combine 2.6, 2.8 and the remark preceeding 2.8. $\square$

We now state a combinatorial principle which is tailored to imply $\text{Con}(T)$. Parts (ii) and (iii) of 2.10 correspond to the similar parts of 2.1. There is no 2.10(i). After showing that 2.10 implies $\text{Con}(T)$, we will return to derive 2.10 from 1.2.

2.10. PROPOSITION. *For all e, k, r there is an M such that for any family $\langle P_\xi; \xi < 2^M \rangle$ of partitions $P_\xi : [M]^e \rightarrow r$, there is an X of cardinality $\geq k$ such that:*

(ii) *if $a, b \in X$ and $a < b$, then $a^2 < b$,*

(iii) *if $a \in X$ and $\xi < 2^a$, then $X \sim (a + 1)$ is homogeneous for P_ξ .*

2.11. CLAIM. 2.10 implies $\text{Con}(T)$.

PROOF. Given a finite subset S of T , let $c_0, \dots, c_{k-1}$ be all constants appearing in S . We will use 2.10 to show that S has a model of the form $\langle \omega; +, \times, <, x_0, \dots, x_{k-1} \rangle$, where $x_0, \dots, x_{k-1}$ are the first k elements of the set X given by 2.10. This model clearly satisfies (i) of 2.1 so we need only worry about those axioms of the forms (ii) and (iii) in S . Part (ii) of 2.10 takes care of the axioms of form (ii) automatically, so we only need to set up our partitions to handle those of form (iii).

We may view each $\xi \in \omega$ as coding a finite increasing sequence $a(\xi)$ from ω in such a way that all sequences from b are coded by some $\xi < 2^b$. Given a limited formula $\psi(y; z)$ and a sequence $a(\xi)$ of the same length as y , we obtain a partition $F_{\psi, \xi} : [M]^{e'} \rightarrow 2$, where e' is the length of z defined by $F_{\psi, \xi}(c) = 0$ if $\psi(a(\xi); c)$, and $= 1$ otherwise.

Consider, for the moment, fixed M and ξ . For each axiom of type (iii) occurring in S there is a corresponding limited formula $\psi(y; z)$ and hence a corresponding partition $F_{\psi, \xi}$. By 2.9 we may combine these into a single partition $P_\xi : [M]^e \rightarrow r$, where e and r depend only on S , not on ξ or M . Now using 2.10, choose M so large that (ii) and (iii) hold for some $X \subseteq M$

for the family $\langle P_\xi; \xi < 2^M \rangle$, and $\text{card}(X) \geq k + e$. Now choosing $x_0, \dots, x_{k-1}$ as described above, we see that all axioms of type (iii) are satisfied. $\square$

Our attentive reader will have noticed that since $\langle \omega; +, \times, < \rangle$ has a primitive recursive satisfaction relation for limited formulas, we can prove in PA (or even PRA) that this structure satisfies (i) of 2.1. Hence the above proof can be carried out in PA.

All that remains is for us to prove (in PA) that 1.2 does imply 2.10. To do this we need a method for obtaining homogeneous sets which grow fast. We are indebted to F. Abramson for some of the following arguments which have simplified our original proof.

For any function g , let $g^{(x)}$ be g composed with itself x times. Let $f_0(x) = x + 2$ and let $f_{n+1}(x) = (f_n)^{(x)}(2)$. The reader can check that $f_1(x) \geq 2x$, $f_2(x) \geq 2^x$, $f_3(x) \geq \beth_x$, where $\beth_x = 2^{2^{\cdot^{\cdot^2}}}$, a stack of x 2's, and so on for $f_4, f_5, \dots$. Readers familiar with the Ackermann function will realize that each f_n is primitive recursive and that every primitive recursive function is eventually dominated by some f_n , but these facts will not be used below.

2.12. LEMMA. *For every p there is a $Q : [M]^1 \rightarrow p + 1$ such that if X is homogeneous for Q and of cardinality at least 2, then $\min(X) \geq p$.*

PROOF. Let $Q(a) = \min(a, p)$. $\square$

We now come to two lemmas which use relatively large homogeneous sets.

2.13. LEMMA. *For each m there is a partition $R : [M]^2 \rightarrow r$ (where r depends only on m) such that if $X \subseteq M$ is relatively large and homogeneous for R and of cardinality > 2 , then for every $x, y \in X$, $x < y$ implies $f_m(x) < y$.*

PROOF. For each $i \leq m$, let $P_i(a, b) = 0$ if $f_i(a) < b$; $= 1$ otherwise. Let $p = f_m(3)$ and let Q be as in 2.12 for this p . Use 2.9 to combine all of these into $R : [M]^2 \rightarrow r$. Let X be relatively large and homogeneous for R . Let $a = \min(X)$, $b = \max(X)$. By induction on $i \leq m$, it is easy to show first that $f_i(a) < b$ (this is where you use $\text{card}(X) \geq a$) and second that $f_i(x) < y$ for all x, y in X , $x < y$, by homogeneity. $\square$

2.14. LEMMA. *Let $P : [M]^e \rightarrow s$ ($e \geq 2$) and m be given. There is a $P^* : [M]^e \rightarrow s'$, where s' depends only on m, e and s , such that if there is a relatively large $Y \subseteq M$ homogeneous for P^* of cardinality $> e$, then there is*

an $X \subseteq M$ such that X is homogeneous for P and $\text{card}(X)$ is at least $e + 1$ and $f_m(\min(X))$.

PROOF. Let $h(a)$ be the largest x such that $f_m(x) \leq a$. For $a = a_1, \dots, a_e$, let $h_a = h(a_1), \dots, h(a_e)$. Let $S(a) = P(h_a)$ if h_a is an e -tuple (i.e., if $h(a_1) < h(a_2) < \dots < h(a_e)$); $S(a) = s$ otherwise. Thus $S : [M]^e \rightarrow s + 1$. Let R be as in 2.13. Use 2.9 to combine R, S into $P^* : [M]^e \rightarrow s'$. Let Y be given as in the statement of our lemma, and let X be the image of Y under h . The partition R promises us that h is one-one on Y so that $\text{card}(X) = \text{card}(Y) \geq \min(Y)$. But the definition of h implies that $f_m(\min(X)) \leq \min(Y)$ so $\text{card}(X) \geq f_m(\min(X))$ as desired. $\square$

2.15. PROPOSITION. *The combinatorial principle of 1.2 implies that of 2.10.*

PROOF. We are given e, k and r , and must produce an M as in 2.10. Find a p so that for all $a \geq p$, $f_3(a)$ is reasonably big as compared with e, r, k and a . We will make this precise in the last paragraph of the proof; for now, just note that $f_3(y) \geq \mathfrak{z}_y$. Let $e' = 2e + 1$.

Now given any M and any family $P_\xi : [M]^e \rightarrow r$ for $\xi < 2^M$, define a new $S : [M]^{e'} \rightarrow 2$ by: $S(a, b, c) = 0$ if $P_\xi(b) = P_\xi(c)$ for all $\xi < 2^a$; $S(a, b, c) = 1$ otherwise. Let Q be as in 2.12 and R as in 2.13 for $m = 2$. Use 2.9 to combine Q, R and S into a single P and then use 2.14 to obtain $P^* : [M]^{e'} \rightarrow s'$. The number s' depends only on $e' = 2e + 1$ and on p . We now apply the combinatorial principle 1.2. Find an M such that $M \xrightarrow{*} (e' + 1)_s^{e'}$. By 2.12 there is an $X \subseteq M$ which is homogeneous for Q, R and S with $\text{card}(X) \geq f_3(\min(X))$. Since X is homogeneous for Q , $\min(X) \geq p$. Since X is homogeneous for R , and since $f_2(y) \geq y^2$ for those y big enough to be in X , X satisfies 2.10(ii).

To verify 2.10(iii), we replace X by $X' = X \sim d$, where $d = d_1, \dots, d_e$ are the last e elements of X . Let $i_\xi = P_\xi(d)$. If we show that for all $a < b_1 < \dots < b_e$ in X' and all $\xi < 2^a$, $P_\xi(b) = i_\xi$, we will have shown that X' satisfies 2.10. To show this it suffices to show that $S(a, b, c) = 0$ for some (hence, by homogeneity, for every) $1 + 2e$ tuple a, b, c from X . Let $a = \min(X)$ and consider consecutive e -tuples from $X \sim (a + 1)$. Our choice of p earlier should be such that there are more than $r^{(2^a)}$ such e -tuples for then we can find e -tuples b, c such that $P_\xi(b) = P_\xi(c)$ for all $\xi < 2^a$, as desired. $\square$

3. Refinements

In the proof of our main theorem we relied on various proof-theoretic results, in particular, on Gödel's Second Incompleteness Theorem. It is possible, however, to prove our main theorem using only model-theoretic methods. This is the approach taken in PARIS [to appear], where a general model-theoretic methodology (called indicator functions) for producing such results is developed.

On the other hand, 1.2 is actually equivalent, in PA, to a well-known proof-theoretic principle, and our proof has the advantage of making this fairly obvious. Recall, from page 849, the definition of RFN_{Σ_1} , the statement of number theory expressing the statement "For all Σ_1 sentences ψ , if $\text{PA} \vdash \psi$, then ψ ".

3.1. THEOREM. *It is a theorem of PA that RFN_{Σ_1} is equivalent to the combinatorial principle of 1.2.*

PROOF. After the proof of 1.2 we mentioned that

$$\text{for all } e, r, k, \text{ PA} \vdash \exists M (M \xrightarrow{*} (k)_e^r).$$

This fact, which we indicated how one would verify, is itself a theorem of PA. An application of RFN_{Σ_1} gives 1.2.

Assume 1.2 and let us prove RFN_{Σ_1} . Let ψ be a Σ_1 sentence. We prove that if $\neg \psi$, then $\text{Con}(\text{PA} + \neg \psi)$. The proof of 2.5 shows that if ψ is false in ω , then $\text{Con}(T + \neg \psi)$, using 1.2. But the proof of 2.2 shows that $\text{Con}(T + \neg \psi)$ implies $\text{Con}(\text{PA} + \neg \psi)$. $\square$

For our final result, define a recursive function f by

$$f(e) = \text{the least } M \text{ such that } M \xrightarrow{*} (e+1)_e^e.$$

3.2. THEOREM. *If g is a (description of a) recursive function, and if $\text{PA} \vdash$ " g is total", then for all sufficiently large e , $f(e) > g(e)$.*

PROOF. Let S be a finite subset of T and let $c_0, \dots, c_{k-1}$ be the constants appearing in S . As the proof of 2.5 (in particular that of 2.11) shows, we may interpret these constants so as to make ω a model of S . By examining that proof, one can see that for all large enough e , we can in fact interpret $c_0, \dots, c_{k-1}$ using members of the interval $(e, f(e))$. If $g(e) \geq f(e)$ for

infinitely many e , the above would show the consistency of T plus the following axioms in a new constant e :

$$e < c_0; \quad \neg \exists x \leq c_i (g(e) \approx x) \quad \text{for all } i \leq \omega.$$

By the proof of 2.2 we obtain the consistency of $\text{PA} + \exists e (g(e) \text{ is not defined})$. $\square$

We wish to thank the editor for almost forcing us to write this chapter, for typing it himself, and for a number of minor changes, provided he accepts responsibility for all misprints.

References

KIRBY, L. and J. PARIS

[to appear] Initial segments of models of Peano's Axioms, in: *Proceedings of the Bierutowice Conference 1976* (Springer, Berlin) to appear.

PARIS, J.

[to appear] Independence results for Peano arithmetic using inner models, to appear.

Index of Names

- Aanderaa, S., 578, 588, 592, 740, 772, 780
Aarts, J.M., 505
Abel, 206, 928, 955
Abramson, F., 1139
Ackermann, W., 1139
Aczel, P., 696, 697, 735, 736, 739, 740, 768,
771, 772, 773, 776, 780
Addison, J.W., 236, 368, 671, 772, 780, 785,
803, 804, 805, 807, 808, 809, 814, 940
Adler, A., 153
Adjan, S.I., 579
d'Alembert, J., 198, 206
Amitsur, S., 124
Aronszajn, N., 384, 385, 386, 394, 395, 398,
472, 473, 474, 484, 499, 500
Artin, E., 131, 132, 141, 146, 148, 149, 151,
152, 609, 1055, 1088
Ax, J., 17, 102, 131, 132, 133, 135, 141, 149,
150, 151, 152, 153, 154, 174, 611, 627

Bachmann, H., 878, 882, 968
Bacsich, P., 122, 135, 143
Baire, M., 159, 365, 369, 377, 379, 380, 492,
497, 501, 504, 505, 506, 785, 798, 813, 928,
1004
Baldwin, J.T., 88, 164
Banach, S., 351, 352, 353, 354, 355, 357, 375,
400, 808, 927, 929
Barendregt, H., 1091, 1093, 1101, 1105,
1117, 1125
Bar-Hillel, Y., 347, 679
Barr, M., 298
Barwise, J., 5, 45, 58, 69, 94, 97, 100, 101, 141,
159, 160, 235, 236, 237, 238, 242, 246, 251,
262, 263, 265, 273, 274, 275, 278, 280, 325,
397, 400, 655, 670, 671, 777, 778, 780, 955,
968
Bastiani, A., 292, 311
Baumgartner, J., 387, 399, 499
Beck, 295
Beeson, M.J., 1022
Behrens, M.F., 207, 209
Berkeley, G., 205
Belegardek, O.B., 164, 169, 170
Bell, J.L., 106, 119, 122, 131, 134, 135
Bénabou, J., 295, 305, 306
Bendixson, I., 84, 85, 749, 784, 955
Bernays, P., 51, 55, 860, 861, 865, 868, 917,
939, 974
Bernstein, F., 353, 516
Bertrand, J., 367
Beth, E., 34, 44, 236, 274, 280, 980, 1024
Bishop, E., 926, 927, 929, 974, 1045, 1046
Blackwell, D., 808
Blass, A., 366
Blum, L., 101, 148, 149, 166
Blum, M., 539
Boffa, M., 171, 175
Böhm, C., 1096, 1101, 1106, 1119, 1120, 1121,
1122, 1123, 1125, 1126, 1131
Boileau, A., 299, 305, 1054
Bolzano, B., 198, 1042, 1043
Boolos, G., 642, 644, 649, 668, 671
Boone, W.W., 169, 578, 579, 580, 593
Borel, F., 358, 377, 498, 750, 753, 785, 787,
915, 917, 925, 928, 929, 955
Boyd, R., 644
Brady, A.H., 533
Bridge, J., 968, 1091
Britton, J.L., 578
Brouwer, L.E.J., 822, 823, 825, 915, 927, 942,
974, 977, 982, 1002, 1005, 1010, 1042,
1044, 1045

- Bruce, K., 100
 Büchi, J.R., 615, 617
 Buchholz, W., 968
 Bunge, M., 299, 310
 Burgess, J.P., 403, 492
 Burkhoff, G., 173
- Comer, S.D., 174
 Cannonito, F.B., 578
 Cantor, G., 84, 85, 203, 206, 207, 253, 261,
 263, 272, 277, 346, 347, 348, 353, 608, 618,
 749, 784, 925
 Carson, A.B., 142, 172, 173
 Cauchy, A., 133, 198, 206, 208, 211, 212, 214,
 215, 219, 563, 925, 926, 928
 Čech, E., 357, 382, 385, 501, 507, 509
 Ceitin, G.S., 564, 1008
 Cenzer, D., 670, 671, 740, 772, 780
 Chang, C.C., 45, 49, 63, 68, 76, 102, 106, 132,
 134, 136, 142, 143, 144, 156, 157, 163, 196,
 277, 280, 487, 488, 757, 780
 Cherlin, G., 159, 172
 Chevalley, C., 295
 Chong, C.T., 662
 Church, A., 51, 235, 533, 534, 535, 541, 564,
 568, 571, 585, 592, 599, 753, 771, 772, 800,
 865, 917, 986, 1007, 1092, 1093, 1095,
 1096, 1100, 1102, 1106, 1120, 1126
 Cobham, A., 51
 Cohen, P.J., 89, 147, 148, 151, 152, 154, 159,
 300, 359, 360, 363, 365, 368, 404, 406, 412,
 414, 420, 421, 423, 424, 427, 451, 606, 628,
 641, 784, 814
 Cohn, P.M., 168, 171, 284, 287
 Cole, J., 308, 310
 Cook, S.A., 600, 627
 Cooper, S.B., 640, 646, 647
 Coste, M., 294, 295, 305, 306, 1054
 Coven, C., 153
 Craig, W., 72, 102, 235, 272, 273, 274
 Curry, H.B., 1092, 1093, 1095, 1101, 1105
- Dalen, D. van, 1025
 Davis, M., 41, 528, 564, 567, 585, 586, 589,
 590, 592, 593, 594, 650, 807, 808, 813, 814
 Dedekind, J., 84, 87, 362, 365, 366, 378, 379,
 380, 385, 386, 925, 926, 954
 Deligne, P., 296
 Demazure, M., 293, 307
 Descartes, R., 289
- Devlin, K., 378, 380, 400, 453, 472, 477, 481,
 484, 488, 489, 514, 517, 518, 521, 522
 Diaconescu, 310
 Diller, J., 1040
 Dionne, J., 295, 296, 305
 Douwen, E. van, 498
 Dowker, C.H., 510, 511
 Dragalin, A.G., 991
 Drake, F., 397, 400
 Dries, L. van den, 173, 174, 179
 Driscoll, G.C., 660
 Dyson, V.H., 1025
- Easton, W., 387, 444
 Ehrenfeucht, A., 98, 182, 184, 186, 187, 189,
 193, 612, 628
 Ehresmann, C., 292
 Eklof, P.C., 97, 105, 127, 136, 141, 155, 158,
 159, 494, 501
 Elgot, C.C., 615, 617
 Enderton, H.B., 527
 Engeler, E., 81
 Engelking, R., 1044
 Ennis, G., 778
 Epstein, R., 647
 Erdős, P., 75, 102, 130, 136, 183, 187, 188,
 378, 392, 393, 396, 401, 484
 Ershov, Y., 17, 132, 136, 141, 148, 149, 150,
 151, 153, 620, 628
 Euler, L., 206, 229
- Feferman, S., 42, 46, 366, 367, 552, 612, 628,
 779, 780, 781, 847, 871, 913, 946, 949, 953,
 955, 961, 962, 965, 968
 Fenstad, J.E., 143, 162, 169, 599, 622, 625,
 628
 Fisher, E., 143, 162, 169
 Fitch, F.B., 34
 Fitting, M.C., 980, 981, 1024
 Floyd, 580
 Fourman, M.P., 305, 1053, 1054, 1060, 1070,
 1081, 1088
 Fraenkel, A.A., 15, 51, 55, 237, 309, 347, 361,
 362, 363, 364, 365, 370, 404, 454, 547, 637,
 784, 815, 840, 1092
 Frege, G., 6
 Frenet, F.-J., 225
 Freyd, P., 288, 295, 307
 Fried, M., 154

- Friedberg, R.M., 554, 564, 639, 645, 650, 661, 669, 670
 Friedman, H., 270, 280, 670, 672, 779, 781, 808, 814, 929, 950, 956, 965, 966, 968, 992, 994
 Frobenius, F., 295
 Fubini, G., 375
 Fuhrken, G., 68, 100
 Fukuyama, M., 658

 Gabbay, D.M., 620, 621
 Gabriel, P., 287, 289, 290, 291, 292, 293, 307
 Gaifman, H., 141
 Gale, D., 642, 643, 807, 808
 Galvin, F., 389
 Gandy, R.O., 265, 376, 670, 671, 672, 707, 730, 735, 736, 740, 768, 771, 772, 773, 776, 777, 780, 781, 934, 952, 953, 956
 Garavaglia, S., 101
 Gauss, C.F., 198, 205, 206, 217, 218, 220, 221, 225, 226, 227, 228, 229, 289, 346
 Gel'fond, M.G., 1041
 Gentzen, G., 23, 34, 37, 40, 274, 298, 305, 747, 869, 871, 878, 893, 899, 900, 917, 946, 957, 958, 968, 969, 986
 Gillman, L., 75, 130
 Girard, J.-Y., 969, 1040
 Giraud, 299
 Gödel, K., 6, 10, 16, 23, 35, 41, 51, 55, 57, 195, 199, 234, 343, 350, 359, 378, 400, 404, 426, 427, 441, 451, 454, 455, 463, 465, 466, 488, 489, 534, 547, 556, 560, 564, 597, 599, 633, 642, 647, 650, 654, 657, 704, 784, 750, 751, 752, 754, 755, 756, 757, 758, 805, 807, 814, 825, 826, 851, 865, 868, 869, 917, 920, 921, 939, 957, 958, 961, 962, 963, 964, 969, 970, 975, 980, 982, 986, 987, 988, 1005, 1027, 1101, 1106, 1133, 1136, 1141
 Goodman, N.D., 1017, 1040
 Goldrei, D.C., 172
 Gordan, C., 346
 Gratzner, G., 120
 Green, M.W., 533
 Greenberg, M., 153
 Gregory, J., 270, 476
 Grilliot, T.J., 730, 732, 734, 735, 736, 757, 773, 781
 Grothendieck, A., 296, 298, 299, 303, 311, 1055, 1088
 Grzegorzczak, A., 752, 754, 781, 1100, 1106

 Hahn, N., 354, 355, 357, 929
 Hall, P., 284
 Halmos, P., 372, 404
 Halpern, J.D., 366
 Haken, W., 579, 580
 Hakim, M., 302
 Hanf, W., 235, 281, 552, 564, 648, 650
 Hajnal, A., 388, 392, 393, 396, 401, 484, 507, 516, 517, 519, 522
 Harnik, V., 256, 266, 267, 269, 271, 275, 278
 Harrington, L., 643, 662, 671, 672, 675, 734, 735, 736, 771, 774, 781, 1133
 Harrison, J., 277, 952
 Hausdorff, F., 27, 60, 75, 84, 102, 128, 136, 352, 353, 356, 357, 519
 Hatcher, W., 1086
 Hechler, S., 508
 Henkin, L., 23, 28, 30, 31, 32, 33, 36, 39, 57, 58, 78, 102, 297, 671, 757, 860, 864, 865
 Henrard, P., 142, 160, 161
 Henrickson, M., 75, 130
 Hensel, G., 149, 150, 151, 644, 649
 Herbrand, J., 234, 534, 885, 889, 897, 898
 Hermann, G., 126, 127
 Hermes, H., 346
 Herstein, I.W., 117, 124
 Heyting, A., 974, 977, 982, 995, 1070
 Higgs, D., 299, 311, 1070
 Higman, G., 159, 168, 169, 170, 171, 175, 176, 578, 593
 Hilbert, D., 6, 23, 34, 37, 41, 42, 125, 126, 131, 141, 142, 146, 148, 149, 150, 152, 174, 305, 346, 557, 568, 584, 585, 586, 587, 598, 599, 741, 822, 823, 824, 825, 846, 858, 859, 860, 861, 865, 868, 915, 917, 927, 974, 980, 981, 1004
 Hinata, S., 1036
 Hindley, R., 1102
 Hinman, P.G., 672, 678, 696, 735, 736, 740, 781
 Hintikka, J., 249, 251
 Hirschelmann, A., 124
 Hirschfeld, J., 142, 167, 168, 172, 207, 231
 Hopcroft, J., 584
 Hopf, L., 288, 308
 Howard, W., 968, 1011, 1032, 1034, 1036, 1037, 1038
 Hurd, A., 207
 Hyland, J., 1125, 1127, 1128, 1130

 Jacobson, N., 147, 148, 149

- Jarden, M., 154
 Jech, T.J., 345, 363, 367, 370, 387, 401, 432, 452, 672
 Jensen, R.B., 68, 76, 102, 141, 207, 230, 270, 378, 384, 387, 398, 435, 436, 465, 472, 474, 475, 477, 483, 484, 487, 488, 489, 510, 514, 521, 644, 650, 655, 668, 671, 672
 Jockusch, C.G., 641, 643, 644, 648, 649, 650, 669, 672
 Jongh, D.H.J. de, 979
 Johnson, D.R., 207
 Johnstone, R., 310
 Jonsbråten, H., 378, 380, 400, 472, 489
 Jónsson, B., 69, 73, 74, 75, 76, 82, 83, 84, 88, 102, 141
 Joyal, A., 174, 294, 295, 296, 300, 301, 305, 306, 307, 308, 310
 Juhász, I., 383, 390, 503, 504, 507, 508, 514, 516, 519

 Kahr, A.S., 548, 588
 Kaiser, K., 157
 Kanamori, A., 398
 Kaplansky, I., 150, 151
 Karp, C., 97, 98, 99, 102, 235, 236, 281, 465, 489, 627, 628, 655, 670, 671, 672
 Keane, O., 292
 Kechris, A.S., 681, 735, 736, 774, 781, 784, 808
 Kegel, O.H., 120
 Kelley, J., 354
 Keisler, H.J., 3, 44, 45, 46, 47, 49, 68, 88, 89, 98, 99, 100, 102, 106, 132, 134, 136, 141, 143, 144, 159, 161, 163, 196, 203, 207, 231, 235, 270, 274, 275, 277, 280, 281, 757, 780
 Kent, C.F., 855
 Kiefe, K., 153
 Kiehne, U., 154
 Kinder, G. de, 310
 Kino, A., 656
 Kirby, L., 1134
 Kirousis, L., 736
 Kleene, S.C., 235, 236, 264, 265, 273, 281, 528, 534, 535, 537, 545, 562, 565, 633, 650, 656, 681, 682, 692, 693, 701, 709, 711, 712, 713, 715, 716, 717, 718, 719, 720, 721, 722, 723, 727, 728, 729, 730, 731, 732, 733, 735, 736, 752, 753, 754, 765, 771, 772, 778, 780, 781, 785, 788, 799, 800, 801, 803, 814, 870, 884, 917, 921, 936, 940, 944, 950, 951, 952, 953, 956, 1010, 1018, 1023, 1029, 1092, 1100, 1104
 Kleinberg, E., 392
 Kochen, S., 17, 110, 132, 133, 135, 136, 141, 147, 148, 149, 150, 151, 174, 611, 627
 Kock, A., 283, 302, 304, 306, 307, 310, 312
 Kolaitis, P., 736
 Kolchin, E., 167
 Kolmogorov, A., 986
 König, J., 126, 136, 383, 384, 394, 395, 927, 928, 953, 1135
 Kondo, M., 276, 368, 803, 804, 814, 926, 940
 Kreider, D.L., 772
 Kreisel, G., 236, 265, 564, 654, 655, 656, 657, 658, 659, 673, 677, 858, 859, 862, 869, 870, 871, 885, 889, 892, 899, 900, 902, 926, 943, 947, 949, 950, 951, 952, 954, 955, 956, 959, 967, 968, 969, 973, 974, 977, 982, 986, 1011, 1012, 1015, 1025, 1029, 1030, 1032, 1045, 1046
 Kripke, S., 234, 235, 237, 238, 239, 264, 281, 300, 301, 306, 621, 655, 656, 657, 658, 668, 673, 772, 980, 981, 1024
 Krivine, J.L., 899, 974, 1055
 Kronecker, L., 822, 823
 Kueker, D., 277, 281
 Kunen, K., 134, 136, 317, 371, 398, 399, 484, 507, 514, 521, 673, 674, 697, 811, 812, 813
 Kuratowski, K., 235, 354, 798
 Kurepa, G., 428, 431, 432, 437, 442, 443, 488, 520, 521

 Lachlan, A., 88, 89, 102, 164, 632, 636, 645, 646, 647, 650, 675
 Lacombe, D., 564, 951
 Lagrange, J., 206
 Lambek, J., 310
 Landau, E., 224
 Lang, S., 106, 133, 136, 150, 153
 Langford, C.H., 604
 Läuchli, H., 366, 612
 Laurent, P., 150
 Lawvere, F.W., 285, 287, 289, 293, 294, 295, 302, 308, 312, 1054, 1055, 1071, 1086
 Lazard, M., 284
 Lebesgue, H., 358, 365, 369, 377, 400, 498, 784, 785, 788, 798, 815, 915, 917, 927, 955
 Lebeuf, R., 636
 Leggett, A., 662, 668
 Leibniz, G.W., 6, 12, 29, 49, 198, 199, 200,

- 201, 203, 204, 205, 206, 209, 210, 211, 212,
214, 215, 372
Leonard, J., 612
Lerman, M., 636, 650, 661, 662, 668, 670, 671,
674, 675, 678
Lesaffre, 310
Lévy, A., 245, 247, 281, 347, 364, 366, 370,
400, 408, 411, 441, 452, 654, 656, 657, 678,
850, 871, 892, 959
Lewis, H.R., 588
L'Hôpital, G. de, 198
Lie, M.S., 112
Lin, S., 533
Lindelöf, E., 499, 508, 517, 521
Lindenbaum, A., 294, 295, 1070
Lindström, P., 45, 95, 97, 147, 162, 164
Lipschitz, L., 172, 173, 174, 928
Löb, M.H., 845, 846, 848, 855, 856, 858
Loeb, P., 207
Lopez-Escobar, E., 96, 99, 102, 235, 236, 272,
273, 274, 281
Lorenzen, P., 926, 957
Loullis, G., 174
Łoś, J., 48, 52, 62, 63, 66, 82, 102, 112, 136,
142, 156, 157
Löwenheim, L., 10, 12, 23, 33, 44, 45, 47, 49,
63, 64, 65, 66, 67, 68, 71, 81, 95, 97, 100,
140, 165, 236, 245, 247, 256, 262, 374, 406,
487, 505, 618, 620
Lowenthal, F., 671
Luckhardt, H., 934, 969
Lutzer, D.J., 505
Luxemburg, W.A.J., 203, 206, 207, 211
Luzin, N., 377, 379, 401, 785, 790, 798, 804,
815
Lyndon, R.C., 72, 102, 578, 592, 593

MacDowell, R., 79
Machover, M., 207, 231, 654, 655, 656, 657,
675
Macintyre, A., 93, 94, 103, 139, 142, 152, 159,
160, 162, 168, 169, 170, 171, 172, 173, 190,
196, 310, 312
MacIntyre, J.M., 661
MacLane, S., 304, 312, 1055, 1087
MacQueen, D., 734
Mahlo, P., 397, 398, 772, 773
Makkai, M., 98, 233, 235, 275, 277, 278, 281,
297, 298, 302, 305, 312
Makowsky, J.A., 143
Mal'cev, A.I., 10, 42, 48, 61, 103, 121, 137
Malitz, J., 99, 235, 281
Malyhin, V.I., 509, 522
Manevitz, L., 162
Mann, C.R., 1093
Mansfield, R., 277, 281, 807
Marczewski, E., 423
Markov, A.A., 577, 579, 979, 991, 995, 1009,
1021, 1023, 1036
Martin, D.A., 370, 377, 403, 444, 449, 484,
491, 492, 494, 501, 503, 504, 636, 639, 642,
643, 646, 647, 651, 783, 807, 808, 811, 812,
813, 914, 929
Martin-Löf, P., 779, 781, 982, 992, 1102
Máté, A., 396
Matijacevič, Yu. V., 557, 568, 585, 587, 589,
590
McKenna, K., 149
McKenzie, R., 578
McKinsey, J.C.C., 52
Meschkowski, H., 824
Meyer, A.R., 599, 623, 624
Mikkelsen, C.J., 302, 304, 305, 310, 312, 1086
Miller, C.W., 169, 170, 177, 472, 639, 649, 651
Minc, G.E., 973, 982, 1017, 1040
Minsky, M., 584
Mitchell, W., 306, 308, 310, 312, 370, 384
Monk, D., 606
Moore, E.F., 497, 548, 565, 588, 593
Morgan, A. de, 25
Morley, M., 49, 57, 69, 73, 76, 82, 83, 84, 85,
86, 87, 88, 89, 103, 135, 141, 148, 164, 166,
167, 181, 193, 196
Moschovakis, Y.N., 261, 265, 281, 525, 669,
670, 671, 676, 681, 682, 690, 696, 697, 730,
731, 733, 734, 736, 740, 753, 765, 767, 768,
769, 770, 773, 774, 777, 778, 780, 781, 784,
785, 786, 797, 798, 808, 809, 810, 811, 813,
814, 1008, 1022, 1024
Mostowski, A., 44, 98, 100, 182, 183, 184,
186, 187, 189, 193, 201, 247, 309, 361, 362,
363, 364, 365, 367, 612, 618, 628, 629, 752,
754, 969
Mučnik, A.A., 554, 565, 645, 651, 661, 670
Mulvey, C., 310, 312
Mycielski, J., 807, 808, 813
Myhill, J., 553

Nagashima, T., 982
Nahm, 1040

- Neumann, B.H., 122, 159, 168, 169
 Neumann, H., 159, 168
 Neumann, J. von, 372, 530, 536, 806
 Neumer, 520
 Newman, J.R., 205
 Newton, I., 198, 205, 372
 Normann, D., 735
 Novikov, P.S., 276, 368, 578, 579, 593, 803, 804
 Nyenhuis, N., 209

 Orevkov, V.P., 982, 1002
 Orey, S., 78
 Osius, G., 305, 306, 308, 309, 310, 312
 Ostaszewski, A.J., 510, 514
 Oullet, 305

 Paré, R., 1086
 Paris, J., 1133, 1134, 1141
 Paterson, M.S., 584
 Peano, G., 6, 55, 79, 330, 347, 348, 548, 553, 1133, 1134
 Picard, E., 208, 221
 Pierce, R.S., 173
 Pincus, D., 365, 366, 367
 Platek, R., 233, 234, 235, 237, 238, 239, 264, 281, 655, 657, 668, 676, 682, 730, 735, 737
 Plotkin, G., 1099, 1107
 Poénaru, V., 580
 Poincaré, J.H., 915
 Pospíšil, B., 382, 385, 509
 Post, E.L., Post, 530, 535, 551, 553, 554, 558, 565, 572, 573, 574, 576, 577, 580, 581, 583, 584, 633, 645, 646, 650, 651, 670, 678, 735, 740, 754, 781
 Pour-El, M.B., 648
 Praag, P. van, 171
 Prawitz, D., 968, 980, 981
 Presburger, M., 67, 151, 599, 603, 606, 617, 625, 628
 Příkrý, K.L., 387
 Putnam, H., 590, 642, 644, 649, 668, 671, 772, 773, 975

 Quine, W., 1059

 Rabin, M.O., 123, 168, 172, 539, 565, 579, 594, 595, 598, 599, 612, 614, 616, 617, 619, 620, 624, 625, 628
 Rado, R., 183, 187, 188, 357, 392, 393, 396, 533, 565
 Ramsey, F., 183, 187, 390, 391, 392, 399, 400, 500, 643, 917, 928, 953, 970, 1134, 1135
 Rasiowa, H., 1024
 Reid, C., 822, 823
 Reinhardt, W., 398
 Ressayre, J.P., 82, 237, 266, 267, 269, 271, 274, 276, 281
 Reyes, G.E., 159, 281, 283, 295, 296, 297, 298, 301, 302, 305, 310, 313, 1065
 Rham, 208
 Rice, H.G., 545, 562, 563, 565
 Richter, W., 740, 772, 773, 780, 781, 782
 Riemann, G., 198, 206, 213, 214, 580, 927
 Ritt, J., 164
 Robertson, E., 624
 Robinson, A., 12, 48, 49, 54, 58, 62, 71, 72, 89, 94, 99, 100, 103, 123, 124, 125, 126, 130, 131, 137, 140, 141, 142, 144, 145, 146, 147, 148, 149, 151, 152, 153, 154, 155, 156, 158, 159, 160, 161, 165, 172, 174, 197, 198, 199, 203, 205, 206, 207, 215, 222, 231, 300, 301, 313, 585, 586, 587, 589, 590, 609, 610, 629
 Robinson, R.W., 639, 646, 647
 Robitaille-Giguère, M., 305
 Rogers, H., 528, 529, 537, 565, 638, 640, 649, 651, 660, 674, 677, 692, 737, 781, 917, 940
 Rolle, M., 607, 1046
 Rosenlicht, 167
 Rosser, J.B., 534, 840, 841, 842, 855, 1092, 1096, 1102, 1120, 1126
 Rotman, J.J., 578
 Rowbottom, 82, 193
 Rowland-Hughes, D., 143
 Rudin, M.E., 136, 307, 491, 510, 514, 522
 Russel, B., 6, 322, 339, 351, 363, 917
 Ryll-Nardzewski, C., 81, 163, 752, 754, 781

 Sabbagh, G., 117, 122, 137, 141, 154, 158, 171, 175, 178
 Sacerdote, G., 154, 176
 Sacks, G., 49, 85, 103, 141, 148, 164, 270, 528, 554, 565, 632, 635, 637, 640, 641, 642, 645, 646, 647, 651, 654, 655, 656, 658, 661, 663, 665, 668, 669, 670, 673, 674, 675, 677, 678, 735, 737
 Sageev, G., 367
 Samuel, P., 127, 137

- Šanin, N.A., 974, 979, 991
 Šapirovsii, B.E., 507, 509, 522
 Saracino, D., 141, 142, 159, 163, 164, 172, 173, 174
 Sasso, L., 647
 Schlipf, J., 266, 968
 Schoenfield, J.B., 46, 148, 155, 321, 398, 400, 412, 414, 415, 416, 452, 495, 501, 528, 559, 560, 565, 578, 594, 632, 639, 640, 645, 646, 651, 663, 677, 735, 737, 811, 815, 889, 951, 952
 Schönfinkel, M., 1092, 1094, 1095
 Schreier, O., 148
 Schubert, H., 287
 Schütte, K., 868, 869, 871, 877, 893, 946, 949, 957, 968, 982
 Schwichtenberg, H., 867, 891
 Scott, D., 98, 103, 149, 235, 276, 282, 299, 310, 327, 400, 452, 649, 651, 677, 861, 1024, 1054, 1055, 1056, 1060, 1070, 1081, 1091, 1100, 1106, 1107, 1110, 1128
 Scott, W.R., 168, 179
 Sgro, J., 101
 Seidenberg, A., 126, 127, 137, 164, 165, 166
 Serret, J.A., 225
 Shelah, S., 82, 87, 89, 103, 135, 137, 140, 143, 160, 161, 164, 167, 190, 196, 486, 494, 495
 Shore, R.A., 484, 653, 661, 662, 663, 665, 667, 668, 669, 670, 674, 675, 677, 678
 Sierpiński, W., 376, 401, 785, 790, 794, 798, 815
 Sikorski, R., 521, 1024
 Silver, J., 196, 387, 398, 400, 401, 431, 432, 433, 441, 442, 452, 480, 488, 514, 515, 807
 Simmons, H., 142, 143, 155, 161, 163, 170
 Simpson, S.G., 631, 639, 640, 641, 643, 644, 650, 651, 661, 662, 669, 670, 671, 672, 675, 677
 Skolem, Th., 6, 10, 12, 23, 33, 44, 45, 48, 49, 56, 57, 63, 64, 65, 66, 67, 68, 71, 81, 95, 97, 100, 130, 140, 163, 185, 186, 187, 188, 190, 193, 194, 195, 236, 245, 247, 255, 256, 262, 374, 406, 452, 466, 467, 469, 477, 478, 480, 487, 608, 612, 618, 620
 Slomson, A.B., 106, 119, 122, 131, 134, 135
 Smoryński, C., 586, 821, 981, 1024
 Smullyan, R.M., 34, 37, 40, 46, 754, 782
 Soare, R.I., 632, 645, 646, 648, 649, 650, 651
 Sochor, A., 363, 367
 Solovay, R., 299, 365, 376, 398, 400, 441, 445, 446, 451, 452, 494, 501, 504, 641, 649, 805, 806, 807, 811, 813, 815
 Specker, E., 276, 636, 637, 639, 652, 768, 771, 773, 774, 782, 953, 954, 968, 1030, 1038
 Spector, C., 276, 636, 637, 639, 652, 768, 771, 774, 782, 953, 954, 968, 1030, 1038
 Statman, R., 871, 897
 Steele, J., 633, 812, 956
 Steinetz, I., 147, 609
 Steinhaus, H., 813
 Stephenson, R.M., 508, 522
 Stewart, F.M., 429, 430, 642, 643, 807, 808, 814
 Stout, L.N., 310
 Stillwell, J., 656
 Stockmeyer, L., 624
 Stone, A.H., 60, 84, 85, 86, 357, 501, 647
 Strong, H., 950, 1093
 Stroyan, K.D., 197, 206, 207, 211, 215, 217, 221
 Sturm, J.C.F., 148, 149, 152
 Sullivan, K., 207
 Suslin, M.I., 233, 235, 236, 264, 272, 276, 341, 378, 379, 384, 385, 386, 390, 453, 472, 473, 474, 475, 476, 484, 485, 493, 494, 499, 505, 507, 510, 559, 566, 668, 785, 792, 794, 798, 811, 813, 815
 Suszko, R., 63, 102, 142, 156, 157
 Svenonius, L., 81, 261, 282
 Swierczkowski, S., 807, 808, 813
 Szabo, M.E., 310
 Szmielew, W., 611
 Tait, W.W., 265, 869, 871, 899, 900, 902, 949, 956, 957, 958, 959, 960, 961, 966, 1036, 1102
 Taitskin, M., 172
 Takahashi, S., 310
 Takeuti, G., 654, 656, 657, 672, 675, 679, 957, 968, 1042, 1055
 Tall, F.D., 507
 Tarski, A., 6, 48, 52, 53, 54, 55, 62, 63, 65, 67, 103, 119, 131, 140, 143, 145, 146, 147, 152, 156, 179, 235, 351, 352, 353, 356, 367, 375, 596, 606, 607, 608, 609, 618, 629, 671, 844, 847
 Taylor, W., 216, 222, 223, 225
 Tennenbaum, S., 445, 446
 Terjanian, G., 132, 151, 152
 Thiele, E.-J., 309
 Thomason, S.R., 637, 646, 647
 Thompson, R.J., 578
 Thue, A., 571, 572, 575, 576, 577, 580

- Tierney, M., 299, 310, 1055, 1071
 Troelstra, A.S., 819, 871, 891, 973, 974, 980,
 981, 982, 985, 990, 991, 992, 993, 1009,
 1012, 1013, 1014, 1015, 1019, 1020, 1021,
 1025, 1026, 1027, 1030, 1032, 1040, 1042,
 1093
 Tugué, T., 656, 657, 692, 735, 737
 Turing, A., 528, 530, 531, 532, 533, 534,
 535, 536, 537, 538, 539, 540, 541, 542, 543,
 547, 548, 549, 550, 552, 553, 554, 562, 566,
 587, 599, 632, 633, 669
 Tychonoff, A., 27, 28, 350, 356, 618

 Ulam, S., 375
 Ullman, J., 584
 Ulm, 97
 Ulmer, F., 287, 289, 290, 291, 292

 Vaught, R.L., 53, 55, 63, 65, 66, 67, 68, 69, 73,
 77, 79, 80, 81, 100, 103, 135, 140, 141, 143,
 235, 237, 254, 255, 256, 257, 259, 261, 262,
 271, 272, 274, 275, 276, 282, 487, 607, 608,
 609, 612, 628
 Verdier, J.L., 1055, 1088
 Vesley, R.E., 994, 1010, 1018, 1023
 Vitali, 352, 365, 784
 Volger, H., 293, 295, 1087

 Waerden, B.L. van der, 563
 Wadge, W., 633, 812
 Wadsworth, C.P., 117, 1121, 1125, 1126,
 1127, 1128

 Wagner, E.G., 950, 1093
 Wainer, S., 735
 Wang, H., 548, 588
 Waskiewicz, J., 174
 Weglorz, B., 174
 Wehrfritz, B.A.F., 120
 Weierstrasz, K., 198, 206, 550, 1042, 1043,
 1045
 Weiss, W., 508
 Weisspfenning, V., 142, 152, 173
 Weyl, H., 217, 822, 823, 825, 926, 975
 Wheeler, W.H., 142, 167, 168, 170, 171, 172
 Whitehead, A.N., 6, 494, 495
 Winkler, P., 164
 Wood, C., 162, 165, 167, 174
 Wraith, G.C., 288, 304, 310

 Yasuhara, A., 528, 580
 Yates, C.E.M., 632, 637, 641, 645, 646, 647,
 672
 Yoneda, N., 288

 Zariski, O., 127, 302, 307
 Zermelo, E., 15, 51, 55, 194, 237, 309, 347,
 348, 404, 410, 416, 454, 547, 637, 784, 808,
 822, 823, 840, 917, 1071, 1092
 Ziegler, M., 153, 171
 Zilber, B.I., 164
 Zorn, M., 107, 338, 354, 355, 356, 379, 419,
 427, 446, 636
 Zucker, J., 779, 968, 1091

Subject Index*

- A-Finite 241
 - see also* Generalized Finite
- A-Recursive 241
- A-Recursively Enumerable 241
- Absoluteness 408f, 417
- Abstract Model Theory 45
- Acceptable Structure 755
 - , Almost 768
- Adjan–Rabin Theorem 579
- Admissible Fragment 244
- Admissible Hull 246
- Admissible Ordinal 246, 270, 470, 657f, 772
- Admissible Set 239, 470, 655, 774f
- Algebraic Theory 285
- Algebraically Closed Model 121
 - see also* Existentially Closed
- Algorithm 528, 568
 - see also* Recursive Function
- Almost Disjoint Sets 387f
- Almost Recursive 649
 - see also* Hyperimmune
- Alternating Chains, Method of 63
- Amalgamation Property 61, 155
- Analysis 644
- Analytic Set 559
- Analytical Hierarchy 558f
- Analytical Relations and Sets 555, 802
- Antichain Conditions 422f, 429f, 441, 444f
 - see also* CCC
- Antichains 413
- Anti-Cohen PO Set 424
- Apartness 995
- Applications to Algebra
 - see the particular kind of structure,*
e.g., Field, P -adic; Groups, Torsion
- Applicative System 1094
- Approximation of Game Formula 259
 - see also* Stages of an Inductive Definition
- Approximation of Terms in λ -Calculus 1126
- Approximation Theorem of λ -Calculus 1127
- Archimedian Axiom 12, 202
- Arithmetic Universe 307
- Arithmetical Comprehension Scheme 937, 938
- Arithmetical Hierarchy 556f
- Arithmetical Relations and Sets 555f, 802
- Aronszajn Tree 384
 - and Martin's Axiom 499
- Artin's Conjecture 132, 147, 150, 151
- Assignment to Variables 20
- Atomic Formula 18
- Atoms 361
 - see also* Urelement
- Autonomous Progressions of Theories 949, 968
- Axiom of Choice 335f, 347, 454, 463
 - Dependent Choice 358
 - Intuitionistic Choice 986, 987
 - Multiple Choice 365
- Axiomatic Recursion Theory 669
- Axiomatizable 22, 50, 112
- Axioms and Rules for First-Order Logic 34, 35, 37, 39
- Axioms for a Theory 50
- Axioms for L (Open) 101
- Axioms for $L_{\omega_1\omega}$ 99
- Axioms for Set Theory 324

* Entries beginning with a Greek letter are at the end.

- Back and Forth Construction 71
- Baire Property 504, 798
 - and Martin's Axiom 492, 497
- Baire Space 785
- Banach-Tarski Paradox 351
- Bar Induction 942, 954, 956, 1010
- Bar-recursion 1031
- Bar Theorem 1010
- Barwise Compactness Theorem
 - see* Σ -Compactness Theorem for Admissible Fragments
- Barwise Completeness Theorem 236
 - , Abstract Form 262
- Barwise Interpolation Theorem 273
- Basic Formula 74
- Basic Omitting Types Theorem 93
- Basic Stone Space Over $\mathbb{N}$ 84
- Basic Type 74
- Basic Type Over $\mathbb{N}$ 82
- Basically κ -Stable 86
- Basically Saturated 74
- Basic Stability Function 87
- Basic Stability Spectrum 87
- Basis 803
- Beth's Theorem 274
- BHK-explanation 977, 982
- Binary Expansion 998
- Binumerate 838
- Blocking Requirements 615
 - see also* Priority Method
- Böhm Trees 1120
- Bohm's Theorem 1106
- Bold Face Σ , Π , Δ 240
- Bolzano-Weierstrasz Theorem 1042
- Boolean Algebras 54, 89
- Boolean Extension 174
- Boolean Power 163
- Boolos-Putnam Theorem 644, 649
- Borel Hierarchy 788
- Borel Set 750, 787
- Box ($\square$) Principle of Jensen
 - see* Square Principle of Jensen
- Büchi's Theorem 615
- Busy Beaver Problem 533

- Canonical Structure 31
- Cantor-Bendixson Construction 749
- Cantor-Bendixson Derivative 84
- Cantor-Bendixson Rank 85
- Cantor-Bendixson Theorem is False in HYP 955
- Cardinal 336f
 - , Regular 372
 - , Singular 372
 - see also* Large Cardinals
- Cardinality of a Model 63
- Cardinality Spectrum 88
- Cartesian Category/Theory 290, 1056
- Categorical Theory 66, 607
 - , $\aleph_0$ 163
 - , $\aleph_1$ 164
- Category of Definable Types and Definable Total Functions 1065
- Category of Models 114
- Category of T-algebras (Models) 285
- Cauchy's Principle 211
- CCC (Countable Antichain Condition)
 - Partial Orders 492
 - Spaces 390, 492, 493, 505
 - see also* Antichain Conditions
- CH
 - see* Continuum Hypothesis
- Chain Conditions
 - see* CCC, Antichain Conditions
- Chain of Models 55
- Chang-Łos-Suszko Theorem 63, 156
- Character 718
- Characteristic Function 302
- Characteristic of a Field 15
- Characterization Theorem (for Realizability) 989
- Characterization Theorem (for the Dialectica Interpretation) 1035
- Choice Function 335, 347
- Choice Sequences 1005
 - , Elimination of 1012f
- Chromatic Number 486
- Church-Kleene ω_1 772
 - see also* Recursive Ordinals
- Church's Thesis, Extended 989
- Church-Rosser Theorem 1102
- Circular Reasoning
 - see* Vicious Circle Principle
- Classes in Set Theory 338f
- Classifying Topos 301
- Closed Unbounded Set 372f, 407
- Closure and Distributivity Conditions 424f, 429, 434f, 443
- Coalgebras 288
- Code 826, 830f, 835f
- Code (of a Function) 702
 - see also* Index
- Coding of Tuples 536, 693, 702

- Coding Scheme 755
- Cohen Extension 414
- Cohen PO Set 420
- Coherent Theory 296
- Collapsing Cardinals 422, 441
- Collapsing PO Set of Lévy 441
- Collection Principles
 - , Δ_0 - 239
 - , Σ - 240
- Coloring Infinite Maps 28
- Combinatorial Principles 423
 - in L 474, 479, 483
 - see also* Diamond, E-principle, Kurepa Hypothesis, Square, W-principle
- Combinatory Algebra 1094
- Compactness Theorem 10, 59, 118, 356
 - , Proofs of 33, 59, 118
 - for Propositional Logic 26
 - Σ - — for Admissible Fragments 251, 776
- Companion Operator 156f
- Companion of a Spector Class 778
- Compatibility 412
- Complete Formula 79
- Complete R.E. Set 543, 553
- Complete Theory 16, 50
- Completeness Test 66
- Completeness 844
 - , Demonstrable Σ_1 844
 - , Semantic 854
 - , Syntactic 854
 - , ω - 854
- Completeness (of Intuitionistic Logic) 1025f
- Completeness (of the Reals) 999
- Completeness Theorem 22f, 844
 - , Barwise 236
 - , Extended 265
 - for Categories 296
 - for $L_{\omega, \omega}$ 99
 - for $L(\mathbb{Q})$ 44
 - , Hilbert–Bernays 860
 - , Proofs of 36f
 - , Significance of 22f
 - , Statements of 35, 39
- Complexity 539, 899f
- Complexity Class 539
- Complexity of Computation 539
- Complexity of Decision Procedures 621f
- Computability
 - see* Effective Computability
- Computation Record 536, 540
- Computational Complexity 539
 - see also* Complexity
- Computers, Digital 536
- Con_T 828
 - $k\text{-Con}_T$ 853
 - $\omega\text{-Con}_T^G$ 853
 - $\omega\text{-Con}_T$ 853
 - 1-Con_T 852
- Concentrates 691
- Conceptual Completeness Theorem 297
- Condensation Lemma 465
 - see also* Mostowski Collapsing Lemma
- Condition for T 89
- Conjunctive Game Formula 254
- Consequence 10, 51
- Conservation Theorem 858
- Conservative Extension 56, 932
- Consistency Property
 - see* Hintikka Set
- Consistent Theory 16, 50
- Constructibility 318, 359, 455, 642f, 649, 654, 667f
- Constructibility, Axiom of 426, 428, 465
- Constructivism 974
- Constructivism, Naive 974
- Constructivization, Global 1040
- Constructivization, Local 1040
- Context-free Grammars 583f
- Continuity Schema 1006
- Continuous 1000
- Continuous, Uniformly 1000
- Continuous Functionals, Extensional 1029
- Continuous Functionals, Intensional 1028
- Continuum Hypothesis 318, 344, 376, 407, 420f, 424f, 454, 465, 635
 - and Martin's Axiom 493, 494
- Contradiction, Law of 25
- Co-recursively Enumerable 647f
- Corona Problem 207
- Countable Functionals 1029
- Countably Compact Space 508
- Course-of-Values 540
- CRA 974, 990
- Craig Interpolation Theorem 72
 - see also* Interpolation Theorem
- Creative Set 553
- Critical Functions of Ordinals 945
- Cross-section 151, 152
- CTM
 - see* Transitive Sets and Models
- C.U.B.
 - see* Closed Unbounded Set

- Cut-elimination Theorem 40, 875, 882, 888, 898f
 - for Infinitely Long Formulas 957
- Cut Rank 873
- Cut Rule 39, 872

- D1, D2, D3
 - see* Derivability Conditions
- Decidable Model 16
- Decidable Relation 535
 - see also* Recursive Relation
- Decidable Theory 16, 52, 596f
- Decidability in Topology 618
- Ded(κ) 87
- Dedekind Set 362
- Definability Lemma 416
- Definition (in a Structure) 555
- Degree Hierarchies 669
- Degrees, Automorphisms of 638, 641, 646
- Degrees, Homomorphisms of 636f, 641
- Degrees, Isomorphisms of 638, 641, 645
- Degrees, Kinds of
 - α -degrees 633, 660
 - Constructibility 642
 - Cuppable 638f
 - Exact Pairs of 637f
 - High 646
 - Kleene 728
 - Low 646
 - Minimal 636, 638, 640, 647
 - Minimal α 661
 - R.E. 551f, 634, 640, 645f, 648f, 650
 - Splitting 638
 - Turing
 - see* Degrees of Unsolvability
- Degrees of Theories 647f
- Degrees of Unsolvability 550f, 631f
- Degrees, Sets of
 - Determined Sets of 642f
 - First-order Definable Sets of 640f
 - Ideals of 636f, 643, 644, 647
 - Independent Sets of 635f
 - Initial Segments
 - see* Ideals of Degrees
 - Semilattices 634f, 645f
- Degrees, Theory of 639, 640f, 646, 647
- Delta System 389
- de Morgan's Laws 25
- Dense Sets 412
- Density Theorem 645, 661
- Dependent Choice, Axiom of 358
- Derivability Conditions 827, 839f
- Derivation in Gentzen System 37
- Derivative 208, 212
- Determinacy 642f, 808
 - , Axiom of 369
 - , Borel 643, 651
 - , Projective (PD) 642f, 808
- Diagonalization Lemma 827
- Diagram 57
- Dialectica Interpretation 1032f
- Diamond ($\diamond$) 318, 378, 510, 517
 - , Consistency of 438
- Differential 221
- Differential Closure 167
- Diophantine Equations, Number of Solutions of 586f
- Diophantine Relations 585f, 588f
- Direct Limit 142, 143
- Direct Product of PO Sets 438
- Directness 899f, 904f
- Discrete Orderings 603, 604, 610
- Distributivity Conditions
 - see* Closure and Distributivity Conditions
- Doctrine 284, 293
- Dominating Families 496, 497
- Double Negation, Law of 25
- Dowker Space 510
- Downward Löwenheim-Skolem Theorem 64

- EC
 - see* Elementary Class
- EC_Δ Class 50
 - see also* Axiomatizable
- ECF 1028
- EED 293
- E.-M.
 - see* Ehrenfeucht-Mostowski
- E-Principle of Jensen 474, 517
 - , Consistency of 435f
- $E(T)$
 - see* Category of Definable Types and Definable Total Functions
- Eastern Model Theory 48
- Effective Computability 525, 528, 530
 - see also* Recursive Function
- Effective Procedure 528f
- Effectively Enumerable Relation 541
 - see also* Recursively Enumerable

- Effectively Inseparable Sets 842
- Ehrenfeucht–Mostowski (E.–M.)
 - Set 184
 - Theorems 182
- Elementarily Equivalent 22, 50, 641
- Elementary Analysis (Intuitionistic) 982
- Elementary Chain 55
- Elementary Chain Theorem 56
- Elementary Class 22, 50, 112
 - see also* Finitely Axiomatizable
- Elementary Diagram 58
- Elementary Embedding 53, 143, 186
- Elementary Extension 53
- Elementary Formula 253
- Elementary in the Wider Sense
 - see* Axiomatizable *and* EC_Δ class
- Elementary Map
 - see* Elementary Embedding
- Elementary Monomorphism
 - see* Elementary Embedding
- Elementary Relation 253
- Elementary Substructure 53, 185
- Elementary Topos 302
- Elimination Mapping 1015
- Elimination of Quantifiers 55, 146, 147, 152, 155, 600f
- Elimination Theorem, First 1016
- Elimination Theorem, Second 1016
- Embedding Theorem 363
- Empty Theory 51
- Encoding
 - see* Coding
- End-extension 247
- Entity 200
- Enumeration Property 701, 730
- Enumeration Theorem 704, 715
 - see also* Normal Form Theorem
- Enumerative Systems 950
- Envelope 728
- Equality Axioms 29
- Equalizer 1057
- Equation Calculus 656, 899f
- Equinumerous 336
- Equivalent Theories 50
- Erdős–Rado Theorem 183, 392
- Essential Unboundedness Theorem 850
- Euclidean Geometry, Decidability of 596
- Excluded Middle, Law of 25
- Existence and Minimality Lemma 414
- Existence Theorem for Basically Saturated Models 75, 76
- Existence Theorem for Prime Models 80
- Existence Theorem for Recursively Saturated Models 70
- Existentially Closed Model 92, 121, 157f
- Existentially Closed Number Theories 172
- Existentially Closed Skew Fields 171, 172
- Existentially Complete
 - see* Existentially Closed Complete
- Existentially Universal (for a Theory) 162
- Expansion of a Structure 30
- Extension 305
- Extension, Recursive 887
- Extensional Structure 246
- Extensionality Axiom 325
- Extensionality in Finite Types 931
 - , Elimination of 934
- External Set 204

- Fan Theorem 1012, 1017
- Field 15, 69, 72f, 92f, 119f
 - , Algebraically Closed 54, 77f, 92, 93, 146, 147, 608
 - , $\mathbb{C}_i$ 150, 151
 - , Differential 84, 87
 - , Differentially Closed 164f
 - , Finite 153
 - , Laurent Series 150f
 - , Non-Archimedean 12, 199
 - , Ordered 54, 64f, 74f, 94
 - , P -adic 149f, 611
 - , Pseudofinite 120, 611
 - , Real Closed 130, 147f, 609
 - , Separably Closed 153
 - , Skew 171, 172
 - , Valued 133, 149f
- Field Object 306
- Filter 106
 - , Cofinite 107
 - , Principal 107
- Fine Structure of L 476, 644
- *-finite (Star-finite) 213
- Finite Character 61
- Finite Hyperreal
 - Number 202
 - Vector 215
- Finite Intersection Property 107
- Finite Limits 1058
- Finite Products 1055
- Finitely Axiomatizable 22, 50, 119, 647f
- Finitely Generated Class of Functionals 703
- Finitely Generated Model 52

- Finitely Satisfiable 58
- Finite Type Structures 919
 - , Maximal 923
 - , Minimal 924
- Finite Types 1026
- Finitism 974, 978
- FIP
 - see* Finite Intersection Property
- First-Order Arithmetic (Intuitionistic) 982
 - see also* Peano Arithmetic
- First Product Theorem 438f
- Fixed Point 683, 684
- Fixed Point Theorems 856f
 - , Brouwer's 1002, 1044
 - of λ -calculus 1101
 - see also* Recursion Theorem *and* de Jongh's Fix-point Theorem
- Forcing Base 98
- Forcing (Cohen) 300, 318, 360, 414f, 641, 699
- Forcing Conditions 415
- Forcing (Finite Robinson) 90, 159, 160, 170, 171
- Forcing (Infinite Robinson) 159, 161, 170, 171
- Forcing in Infinitary Logic 98
- Forcing Product of PO Sets 439f
- Forgetful Functor 115
- Formally Intuitionistic Systems, Translation into 962
- Formula 19, 405
 - , Atomic 18
 - , Conjunctive Game 254
 - , First-order 19
 - , Minor 872
 - , Principal 872
 - , Side 872
 - , Vaught 254
 - , Δ_0 238, 409f
 - , Π 239
 - , Σ 239
- Fragment 250
- Free Algebra 287
- Free Variable 20
- Friedberg Jump Theorem 638, 639
- Friedberg–Muchnik Theorem 645, 661
 - see also* Post's Problem
- Functional 683
 - , Evaluation 685
 - , Minimalization 686
 - , Normal 697, 714
 - , Operative 687
 - , Primitive Recursion 687
 - , Signature of 683
 - , Substitution 686, 688
- Fundamental Theorem of Calculus 214
- Fundamental Theorem of
 - Ultraproducts 112
- Galaxy 204
- Gale–Stewart Games 642
- Game Form Theorem 256
- Games 748, 769
 - see also* Conjunctive Game Formula, Determinacy, Gale–Stewart Theorem
- Gandy–Kreisel–Tait Theorem 265
- GCH
 - see* Generalized Continuum Hypothesis
- Geometric Morphism/Functor 300
- Generalization Rule 32
- Generalized Continuity 1019
- Generalized Continuum Hypothesis 407, 454, 465
 - , Consistency of 426
- Generalized Finite 655, 657, 658
 - see also* A-finite
- Generalized Suslin Hypothesis 473
- Generated Substructure 52, 184
- Generic Circle 292
- Generic Extension
 - see* Cohen Extension
- Generic Model Theorem 91, 99
- Generic Sets 90, 99, 360, 413
- Generic Structure 288
- Gentzen's Theorem
 - see* Cut-elimination Theorem
- Geometric Morphism 300
- Gödel Completeness Theorem 32
- Gödel's Functional (or Dialectica) Interpretation 963, 1035
- Gödel Incompleteness Theorem 560, 599
- Gödel Numbering 547, 633, 647
- Good Ultrafilter 134
- Graphs 486
- Grothendieck Topos 298
- Groups 8, 62, 76, 94f
 - , Abelian 8, 611
 - , Divisible 8
 - , Existentially Closed 168f
 - , Free 54, 97
 - , Galois 72
 - , Linear 121
 - , Matrix 62

- , Orderable 62
- , Solvable 62
- , Torsion 9, 94, 97
- , Torsion-free 9
- , Universal Locally Finite 190
- , Z- 151
- see also* Whitehead's Problem
- Groups and Unsolvability Problems 578f

- $H(\kappa)$, $H_U(\kappa)$ 244
- Hahn-Banach Theorem 354
- Halting Problem 538, 569
- Hanf's Theorem 648, 650
- Handbook, Cost of
 - see* Large Cardinals
- Henkin Axioms 30
- Henkin Construction 31
- Hensel's Lemma 149, 150
- Herbrand Normal Form 889
- Herbrand's Theorem 876, 898f
- Hereditarily Continuous Functional 951
- HEO
 - see* Hereditarily Effective Operations
- Hereditarily Effective Operations 1028
- Hereditarily Finite Sets 43
- Hereditarily Hyperarithmetic Operations 952
- Hereditarily Recursive Operations 951, 1027
- HFD Set 515
- Hierarchy Theorem 558f
- Higher-order Language 7, 43, 1060
- Higher Type Objects
 - see* Object of Higher Type
- Hilbert's Basis Theorem 126
- Hilbert's Program 822f, 868
- Hilbert-Bernays Completeness Theorem 860
- Hilbert's Nullstellensatz 125, 146
 - see also* Nullstellensatz
- Hilbert's 17th Problem 148, 149
- Hilbert's Program 598
- Hilbert's Tenth Problem 568, 584f
- Hilbert's Thesis 41, 587
- Hintikka Set 250
- Homeomorphism Problem 579f
- Homogeneous Linear Ordering 65
- Homogeneous Model 75
- Homogeneous-universal Structures 141, 161
- Homogenous Set 183, 193
- Homomorphic Image 72
- Homomorphism 72, 108
 - of λ -algebra 1100
- Hopf Algebra 288, 308
- HRO
 - see* Hereditarily Recursive Operations
- Hyperarithmetical Hierarchy 559, 753
- Hyperelementary 767
- $HYP(a)$, $HYP(\aleph)$ 245, 246
- Hyperimmune 651
- Hyperinteger 202
- Hyperjump Hierarchy Comprehension Schemes 947
- Hyperreal Numbers 200, 202

- ICF 1028
- Ideal 13, 355
 - , Prime 14
 - , Maximal 14
- Ideal Statements 823
- Image (Homomorphic) 72
- Immediate Extension 150
- imp 826, 836
- Inaccessible Cardinal 343, 396
- Inclusion 310
- Incompleteness Theorem
 - , First 825, 827, 845, 861
 - , Formalized First 852
 - , Second 825, 828, 846, 862
 - , Formalized Second 828
- Independent Theory 88
- Index (of a Function) 538, 702
 - see also* Code
- Index (of the Handbook)
 - see* Self-reference
- Index Transfer Method 724, 726, 728
- Indicator Function 1141
- Induction 739f
 - , Positive Existential 761f
 - , Positive Elementary 764
 - , Non-monotone 774f
- Induction Completeness Theorem 690
- Induction
 - on TC 243
 - on Sets 334
 - on Ordinals 331f
 - , Transfinite 878, 942, 1011
 - , on Unsecured Sequences 1009
- Inductive Definitions 526
 - , Dual of 749
 - , Theories of 968
- Inductive Theory 55

- Ineffable Cardinal 399, 488
- Infinite
 - Hyperreal Number 202
 - Integer 202
- Infinite Derivation 880
 - , Code for 886
- Infinite Telescope 204
- Infinitesimally Close 202
- Infinitary Logic 43, 97f, 244f
- Infinitesimal
 - Number 12, 198, 202
 - Vector 215
- Infinitesimal Analysis 197f
- Infinitesimal Calculus 207, 208f
- Infinitesimal Microscope 203
- Infinite Terms 959
 - , Normalization of 960
- Infinity Axiom 326
- Instantaneous Description 536
- Integral 213
- Integral Definite Functions 152
- Iteration Theorem
 - see Parameter Theorem
- Intermediate Value Theorem 1001, 1042f
- Internal Quantification 304
- Internal Set 199, 204, 265
- Interpolation Theorem 72, 272
 - see also Robinson Consistency Theorem, Suslin Separation Theorem
- Interpretation of λ -terms 1098
- Interpretation
 - of a Language in a Topos 1076
 - of One Theory in Another 598, 612f
 - of Terms of Forcing Language 413
- Intuitionism 974
- Inversion Lemma 873, 881, 887
- Isolated Type 79, 82
- Isomorphic Embedding 53
- Isomorphism 53, 109
- Iteration of Forcing
 - see Products of PO Sets and Martin's Axiom
- J
 - see L and Oracle
- Jensenlehre
 - see Fine Structure of L
- Joint Embedding Property 73, 160, 161
- de Jongh's Fix-point Theorem 856f
- Jónsson Theory 73
- Jump
 - , Iterating 634, 644, 636
 - Theorems 638f
 - Operator 551, 558, 634, 638f, 645, 670
- Jump Hierarchy Comprehension Schemes 947
- k-consistency 853
- Kaiser Hull 157
- Kent's Theorem 855
- Kernel 361
- KH
 - see Kurepa Hypothesis
- Kleene Class of Functionals 709
- Kleene Recursion in Type 2 Object 692
- Kleene Recursive (Higher Types) 711
- Kleene Recursive in 728
- KPU 239
- Kripke-Joyal Semantics 300
- Kripke-Platek Axioms 239
- Kurepa Hypothesis, Consistency of 428f, 437f
 - , Independence of 442
- Kurepa Tree 428, 488, 521
- L
 - see Constructibility
- L-space 517
- L-structures
 - see Model
- L_A 244
- L_{∞} -equivalent 97
- Lambda Calculus 534
- Lambda Definability 534f
- Large Cardinals 342, 396f
 - see also Ineffable Cardinal, Mahlo Cardinal, Weakly Compact Cardinals, Inaccessible Cardinal, Measurable Cardinal
- Lattice of α -Recursively Enumerable Sets 662
- Lattices in Degree Theory 634f, 645f
- Lawless Sequences 1019f
- Lawlike Operations 1027
- Least Upper Bound 1001
- Leibniz' Principle 198, 200
- Lévy Absoluteness Theorem 245
- Light Face Σ , Π , Δ 240
- Limit Recursive 634
- Lindenbaum Doctrine 294
- Lindström's Theorem 45
- Linear Order 64f, 75, 82f

- Linear Order, Second-order Theory of 617
- Linearly Ordered Sets, Decidability of 612
- Löb's Theorem 845, 848
 - , Formalized 855, 858
- Local System 120
- Localization 298
- Logic
 - , Effectiveness in 546
 - , First-Order 6f, 587, 588
 - , Infinitary 43, 97f, 244f
 - , Modal 620
 - , Non-classical 620
 - , Second-Order 7
 - , Weak Second-Order 43
 - with new Quantifiers 43
- Logical
 - Category/Morphism 295, 296
 - Consequence 10, 51
 - Functor 1085
 - Morphism 296
- Lopez-Escobar's Theorem
 - see* Interpolation Theorem
- Łos' Theorem
 - see* Fundamental Theorem of Ultra-products
- Łos-Tarski Theorem 156
- Łos-Vaught Test 66
- Löwenheim-Skolem Theorem 10, 63, 64, 65, 374
- L.U.B. Principle is False in HYP 954
- Luzin Set 377
- Lyndon Homomorphism Theorem 72

- MA
 - see* Martin's Axiom
- Mahlo Cardinal 397
- Many-one Reducibility 544
- Many-sorted Logic 42, 49
- Markov's Rule 1036
- Markov's Schema 990, 1021f, 1025
- Martin's Axiom 318
 - , Consistency of 444f
 - , Uses of 491f, 504f
- Matijasevič's Theorem 557
- Maximal Sets 646
- Measurable Cardinal 344, 400, 806
- Measurable Set 798
- Measure and Martin's Axiom 498
- Metrizible Space 518
- Minimal Pairs 661
- Minimal Model 166, 167, 170
- Model (Structure, L-Structure) 17, 50
- Model Companion 154f
- Model Complete Theory 54, 130, 144f
- Model Completion 141, 154, 155, 165, 166
- Model Pair 71
- Model of λ -calculus
 - see* λ -algebra
- Modules 87
- Modulus of Continuity 890
- Monic 1057
- Monoids 66
- Monomorphism 1057
- Monotone Operator 683, 731, 744
- Morley Categoricity Theorem 82
- Morley Expansion 57
- Morley Rank 83, 84
- Morphism 286
- Mostowski Collapsing Lemma 201, 247, 309, 465
- Multiply Ordered Theory 88

- Natural Numbers 330, 528
 - see also* Peano Arithmetic
- Natural Number Object 1086
- Near-standard 203, 216
- neg 826, 836
- Negation Normal Form 249
- Negation (or Double-negation)
 - Translation 962, 985
- Negative Formula 985
 - , Almost 988
- Neighbourhood Function 1008
- Next Admissible Set 245, 777
- N.N.F.
 - see* Negation Normal Form
- No Counterexample Interpretation 870
- Non-principal Ultrafilter 108
- Non-standard Analysis 231
- Norm 700, 765
- Normal Class of Functionals 697
- Normal Form Theorem 537, 541
- Normal Sequence of Functionals 699
- Normalization Theorem of Curry 1105
- Normed (Class of Relations) 700
- Nowhere Dense Set 496, 497
- Normed Pointclass 730
- Nullstellensatz 125, 146, 147, 153, 167, 171
- Number Selection Lemma 706
- Number Theory in Finite Types 934
- Numeralwise Representability 838
- Numerate 838

- Object of Higher Type 669f, 692, 707, 740
- Omitted Type 77
- Omitting Types Theorem 78
- One-One Reducibility 544
- One-type 189
- Operation 285
- Operation Symbol, Σ - 241
- Operative Functional 684
- Oracle 540, 633
- Ordered Pair 329
- Ordered Theory 88
- Ordinal Notations 562, 752, 771, 968
- Ordinals 330f
 - see also* Admissible Ordinal, Recursive Ordinals, Ordinal Notations
- Ostaszewski Space 510

- $P = NP$ Problem 600, 625
- Parameter Theorem 544f
- PA
 - see* Peano Arithmetic
- Parameterization 763
- Paris-Harrington Theorem 1134
- Partial Elements 1058f
- Partial Function 528
- Partial Isomorphism 97
- Partial Map 1074
- Partially Ordered Sets 407, 412f
 - and Martin's Axiom 496
- Partition Calculus 390f, 484, 1134
- PD
 - see* Determinacy
- Peano Arithmetic 79, 330, 840, 851, 860f, 1134
- Perfect Kernel 85
- Perfect Set 382, 784
- Perfect Subset Property 798
- Perfect Subset Theorem 277
- Permutation Models 361
- Persistence Property 239
- P.G.
 - see* Point Generator
- Phrase Structure Grammars 582
- PO Sets
 - see* Partially Ordered Sets
- Point 708
 - , Arity of 716
 - , Character of 718
 - , Type of 707
- Point-Generator 1003
- Point Projection 710
- Pointclass 785
 - , Properties of 730
- Pointset of Type k 728
- Polish Space 785
- Polynomial Time 627
- Positive Formula 72
- Post Canonical Systems 755
- Post Correspondence Problem 580
- Post's Problem 554, 645f, 661
- Post's Theorem 558
- Post Words 572f
- Power Set 328
 - Axiom 326
- PRA** 840, 859
- Predicate Calculus, Intuitionistic 980
- Predicates on Admissible Sets (Σ , Δ , Σ , Δ) 240
- Predicativity 949, 968
- Presburger's Arithmetic 603, 606, 617, 625
- Preservation of Cardinals 422f, 425f, 443f
- Pressing-down Lemma 374
- Pretopos 297
- Prewellordering 700, 796
 - Property 700, 730
 - Theorem 700
- Pre- λ -Algebra 1098
- PR Formula 843
- Prime Formulas 23
- Prime Ideal Theorem 356
- Prime Model 80, 145, 165, 166, 167, 170, 610
- Primitive Recursion
 - Functional 681, 884
 - Test 145
 - , $< \epsilon_0$ -Recursive 884
- Primitive Recursive 534
 - Function 831
 - Formula 843
- Priority Method 554, 640, 645f, 648, 661
- Productive Function 553
- Products of PO Sets 438f
- Program 528
- Progression Rule 879
- Projection 686, 789
- Projective Determinacy
 - see* Determinacy
- Projective Plane 306
- Projective Set 790
- Projectum 478, 666, 668
- Proof 32
- Proofhood, Decidability of 546f
- Proof-search Procedure 898f, 904f

- Propositional Logic 23
- Prov_T 826, 837f
- Pr_T 826, 838
- Pr_T^R 841
- Pseudo-elementary Class 116
- Pullback 1057

- Quantification Operators 935, 936
- Quantifier 44, 694, 769, 770
 - , Bounded 200
 - , Dual of a 695, 770
 - , Existential 695
 - , Game 769
 - , Monotone 770
 - , Suslin 695
 - , Universal 695
- Quantifier Axioms 30
- Quasi-disjoint
 - see* Delta System

- RA
 - see* Recursive Analysis
- Rado Selection Lemma 357
- Ramified Analysis 948
- Ramified Analytic Sets 948
- Ramified Progressions of Theories 949, 968
- Ramsey Theorem 183, 392
 - , Finite 392
 - , Extension of the Finite 393
- R.E.
 - see* Recursively Enumerable
- Real Number Generator 993
- Realizability 987f, 1018
- Realize a Type 77, 266
- Realized Type 77
- Real Numbers, Non-axiomatizability of 11
- Real Statements 823
- Recursion in Set Theory 333
- Recursion (Σ) 243
- Recursion on Ordinals
 - see* α -Recursion
- Recursion Operators 933, 936
- Recursion Theorem 545, 690, 705, 716
- Recursive Analysis
 - , Classical 975, 991
 - , Constructive 974, 990
- Recursive Analogues of Transfinite Number Classes 772
- Recursive Function 529, 531, 560f, 632, 634, 649, 740, 754
 - , General 534
 - , Primitive 534
- Recursive Functional 540f
 - of Finite Type 709, 952
- Recursive Language 50
- Recursive Operator 563f
- Recursive Ordinals 559, 561f
 - see also* Church-Kleene ω_1
- Recursive Real Numbers 562f
- Recursive Relation 305, 532
- Recursive Set 532, 800, 842
- Recursively Axiomatizable Theory 50, 547f, 552
- Recursively Enumerable 542f, 552f, 570, 750, 800, 841
- Recursively Saturated Model 69
- Redex 1102
- Reduced Product 109
- Reducibility
 - , Many-One 544
 - , One-One 544
 - , Turing 550
 - see also* Relative Recursiveness and Degrees
- Reduct of a Structure 30, 115
- Reduction 276, 795
- Reflection Principle (Σ) 240
- Reflection Principle (Proof Theoretic) 892
 - , Local 845f
 - , Uniform 845f
- $\text{RFN}'(\mathbf{T})$ 845
- $\text{RFN}'_{\Pi_1}(\mathbf{T})$ 846
- $\text{RFN}'_{\Sigma_n}(\mathbf{T})$ 849
- $\text{RFN}'_{\Pi_n}(\mathbf{T})$ 849
- $\text{Rfn}(\mathbf{T})$ 845
- $\text{Rfn}_{\Pi_1}(\mathbf{T})$ 846
- $\text{Rfn}_{\Sigma_n}(\mathbf{T})$ 849
- $\text{Rfn}_{\Pi_n}(\mathbf{T})$ 849
- Reflexiveness Theorem 851
- Reflexive Theory 851
- Regular Cardinal 372
- Regular Category 295
- Regular Set 665
- Regularity Axiom 326
- Relative Admissibility 242
- Relative Consistency 404
- Relative Consistency Theorem 859
- Relative Recursiveness 540, 549f, 633f
 - see also* Relativization
- Relatively Algebraically Closed 144

- Relativization 638, 639, 648f
 - see also* Relative Recursiveness,
 - Recursively Enumerable, Roger's Conjecture, Reducibility
- Relativization of Notions to Universes 924
- Remarkable E.-M. Set 194
- Replacement (Σ , Σ_1) 241, 658
- Representability 751, 753f
- Representing Function 831
- Resolvable Admissible Set 270
- Restricted Induction 931, 967
- Restriction of a Functional 691
- RFN
 - see* Reflection Principle (Proof Theoretic)
- Rice's Theorem 545f
- Rings
 - , Division 110, 124
 - , Local 296
 - , Prime 123
 - , Primitive 117, 124
 - , Principal Ideal 14
 - of Polynomials 54, 97
 - , Regular 172f
 - , Regular f 173f
- Robinson Consistency Theorem 71
 - see also* Interpolation Theorem
- Robinson's Test 144f
- Roger's Conjecture 638
- Rolle's Theorem 1046
- Rosser's Theorem 841
 - , Formalized 854
- Rules for First-Order Logic
 - Hilbert-style 31
 - Gentzen-style 37, 872
- Rules for $L_{\omega, \omega}$ 99
- Rule Set 741
 - , Finitary 742
 - , Deterministic 744
 - , Recursive (r.e.) 751
 - , Regular Arithmetical 752
 - , Regular Elementary 757
- S-Space 516
- Satisfaction Relation 20f
- Satisfiable 50, 69
- Saturated Model 76, 128, 134, 147
 - , Σ - 266
 - , Recursively 69
- Scale 810
- Schemata in Finite Type Theories 932
 - , Comprehension 933, 938
 - , Choice 933, 935, 938
 - , Second-Order 937
- Second-Order Arithmetic 168, 639f
 - see also* Analysis
- Second-Order Arithmetic (Intuitionistic) 983
- Second Product Theorem 440
- Section 729
- 1-Section of Relative Primitive Recursive Functionals 961
- Self-reference 1162
- SemComp_r 854
- Semi-decidable Relation 541
- Semigroups 576
- Semi-recursive Relation 542f, 693
 - see also* Recursively Enumerable
- Semi-recursive Set 542f, 693, 800
- Semi-Thue Processes 571f, 581f
- Sentence, First-Order 20
- Separation Axiom 325
- Separation Schema 321f
 - , Δ_0 - 239
 - , Δ - 241
- Seq 834
- Sequent 37
- Sequentially Compact Space 509
- Set Mappings 485
- Set Theory, Axioms for 15, 321f
- Set Theory, Consistency of 654
- Sheaf 172f, 298
- Signature of a Functional 683
- Simple Model 122
- Simple Set 553
- Simplified Form of a Point 716
- Simultaneous Induction Lemma 687
- Site 298
- Skolem Expansion 57, 164, 185
- Skolem Function 57, 185
- Skolem Paradox 406
- Skolem Relation 56
- Skolemization 164
- Skolem Term 185
- S - m - n Theorem 544, 705, 715
- Solvable Term of λ -Calculus 1117
- Soundness Lemma 35
- Sound Theory 827, 844
- Souslin Line
 - see* Suslin Line
- Space, Metric (Intuitionistic) 1002, 1003
- Spector Class 767, 777
- Spector-Gandy Theorem 276
 - , Abstract Version of 768

- Speed-up Theorem 539
- Splitting Theorem 663f
- Square ($\square$) Principle of Jensen 479
 - , Consistency of 434f
- Stable Ordinal 246
- Stable Theory 87, 164, 173, 192
- Stage Comparison Partial Function 696
- Stage Comparison Theorem 697, 766
- Stages of an Inductive Definition 758
- Stages (for Constructing Sets) 323
- Standard Codes 478
- Standard Part 203, 215
- Standard Representation 1003
- State 530
- Stationary Set of Ordinals 372f, 407
- Steinitz Theorems 147, 149
- Stone Space of a Language 59
- Stone Space over a Model 84
- Strategy 643
- Strong Relation Universality 267
- Structure 17
 - see also* Model
- Structure Induced by an Interpretation 613
- Sturm's Theorem 148
- St(x) 203
- Sub 826, 836f
- Subformula 95
 - Property 876
- Subobject Classifier 1068
- Substructure (Subsystem) 52, 184
- Subsystem
 - see* Substructure
- Suitable Class 685
- Superjump 735
- Superstable Theory 87
- Superstructure 200
- Support 237, 361
- Suslin
 - Hypothesis 472, 484
 - Line 378
 - Property
 - see* CC Spaces
 - Quantifier 695
 - Separation Theorem 272, 559, 792
 - Set 811
 - Tree 385, 472, 473
 - and Martin's Axiom 499
- Symbol 7
- Symmetric Extension 360, 362
- SynComp_T 854
- Systems of Notations for Ordinals
 - see* Ordinal Notations
- TC
 - see* Transitive Closure
- T-predicate 537, 541
- Tarski's Decidability Theorem for the Reals 596, 606, 609, 624
- Tarski's Undefinability Theorem 558
 - see also* Truth in Arithmetic
- Tautology
 - of Propositional Logic 25
 - of First-Order Logic 28
- Taylor's Small Oh Formula 216
- Term
 - , Closed 18
 - , of Forcing Language 413
 - , Skolem 185
- Theory 50
 - , Complete 16
 - , Consistent 16
 - , of a Class K 50
 - , Decidable 16
- Thue Processes 575
- Topology, Unsolvable Problems in 579f
- Topos 298, 1054, 1068
- Total Function 528
- Totally Transcendental 84
- Transfinite Induction Scheme 942
 - see also* Induction
- *-Transform 199, 200f
- Transition Function 531
- Transitive Closure 242
- Transitive Collapse
 - see* Mostowski Collapsing Lemma
- Transitive Set Object 309
- Transitive Sets and Models 405f
- Transitivity Theorem 559
- Tree 381f, 407, 472
 - see also* Aronszajn Tree, Suslin Tree
- Tree Decidability Theorem 616
- Tr_M 860f
- Tr_n 844, 850
- Truncation Lemma 248
- Truth
 - Assignment (for Propositional Logic) 24
 - (in Arithmetic) 558, 560, 639, 647
 - Definition 843
 - Lemma 415
 - Set of Arithmetic 639, 647
 - Table 24
- Tugué Object 692
- Turing Machine 530f, 569f, 587, 590f
 - , Universal 536

- Turing Reducibility 550, 633
 - see also* Relativization
- Two-cardinal Models 68
- Two-cardinal Theorems 68, 487
- Type 76, 127
 - , Σ Family of 266
 - (Definable) 1064
 - of a Point 707
 - Symbols 929
- Ulam Matrix 376
- Ultrafilter 107
 - , Good 134
 - , Principal 108
- Ultrapower 109
- Ultraproduct 109f
 - of Rings 110
- Uncountability Quantifier 44
- Undecidable Theory 16, 548, 597
- Unfruitful Limitations on Mathematics 330
- Uniformization Theorem 368, 803
- Uniformly Continuous 206
- Uniformly Differentiable 206, 208
- Union Axiom 326
- Uniqueness Theorem for Prime Models 80
- Uniqueness Theorem for Basic Saturated Models 75, 76
- Universal
 - Formula 52
 - Function 702
 - R.E. Relation 543
 - Set 788
 - System 705, 715
 - Theory 53
 - Turing Machine 536
- Universes of Sets and Functions 918
 - , Cartesian Closed 921
 - , $\mathbf{N}$ -closed 921
 - , $\exists^{\mathbf{N}}$ -closed 921
- Unsecured Sequences, Induction over 1009
- Unsolvable Problems 534, 538, 545, 548
- Unstable Theory 87
- Upward Löwenheim-Skolem Theorem 65
- Urelement 237, 322
- $V = L$
 - see* Constructibility, Axiom of
- Valid 29
- Validity (Intuitionistic) 1024f
- Value Category 286
- Vaught Covering Theorem 271
- Vaught Formula 254
- Vaught Reduction Theorem 276
- Vicious Circle Principle
 - see* Circular Reasoning
- W-Principle of Silver 514
 - , Consistency of 432f
- Weak α -recursiveness 660
- Weak Counterexample 996
- Weak Robinson Forcing 90
- Weakly Compact Cardinals 397, 483
- Weierstrasz' Approximation Theorem 1045
- Well-founded Relation 305, 743
 - , Length of 792
 - of Orderings 941
 - Part 247
 - Structure 246
 - Tree 747
- Well Ordered Model 193
- Well-orderings 96
 - , Comparability of 945, 954
 - , Provably Recursive 945
 - of $\mathbf{Z}$ 946, 958
 - of Ramified Analysis 959
 - , Natural 878
- Well-ordering Theorem 347
- Western Model Theory 48
- Witnessing Constants 30
- Whitehead's Problem 494
- Witnessing Expansion 29
- Word Problem 169, 171
 - for Semigroups 577
 - for Groups 578
- $\mathbf{Z}$ -group 151
- Zariski Topos 302, 307
- Zermelo-Fraenkel Axioms for Set Theory 324f, 404, 840, 851
- ZF
 - see* Zermelo-Fraenkel Axioms for Set Theory
- ZFC
 - see* Zermelo-Fraenkel Axioms for Set Theory
- ZO Set Theory 309
- Zorn's Lemma 338, 355

- α -Calculability 659
- α -Finite 657f
 - see also* A-finite
- α -Recursion 653–679, 885
- α -Recursive 656–658
- α -Recursive in 660
- α -Recursively Enumerable 656–658
- $\in$ -Model 64
- η_0 -Set 128
- η_1 -Set 129
- λ -Algebra 1099
 - , Weakly Extensional 1099
 - , Extensional 1099
 - , Interior of a 1100
 - , Hard 1100
 - , Sensible 1119
- λ -Calculus 1092f
- λ -Definable Functions 1103
- Λ 828
- π -Complete Space 505
- π_1, π_2 830, 834
- Π_1^1 Relations 752
- Π_n Formula 843
- Σ -Compactness Theorem for Admissible Fragments 251, 776
- Σ_n Formula 843
- φ_f 838
- ω -Comp_T 854
- ω -Complete Theory 78
- ω -Completeness Theorem 78
- ω -Consistency 825, 851f
 - , Local 853
 - , Uniform 853
 - , Global 853
- ω -Homogeneous Model 70
- ω -Logic 42
- ω -Parametrization (of a Class of Functions) 702
- ω -Parameterized Pointclass 730
- ω -Pseudo Complete 133
- ω -Rule 78, 752, 878
- ω_1 -Incomplete Ultrafilter 129
- ω_1 -Saturated 128
- Ω -Set 1070